CONFERENCE ON CYBER CONFLICT

PROCEEDINGS 2010

Edited by
Christian CZOSSECK
and
Karlis PODINS

15.-18. JUNE 2010, TALLINN ESTONIA

Version 1.0 June 2010

ISBN: 978-9949-9040-1-3

Publisher:
CCD COE Publications
Filtri Tee 12, 10132 Tallinn, Estonia
Tel: +372 717 68 00
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org

Printed By:
Ecoprint AS,
Savimäe 13, 60534, Tartumaa

Cover Design: Viljar Väli
Cover Finishing: Jaakko Matsalu
Content Layout: Marko Söönurm

FOREWORD

The CCD COE Conference on Cyber Conflict is a fusion of two highly successful events hosted by the Cooperative Cyber Defence Centre of Excellence (CCD COE) in 2009. Both the Conference on Cyber Warfare and the International Cyber Conflicts Legal and Policy Conference looked at various aspects of Internet-mounted attacks against states or critical state assets.

To support CCD COE's mission of enhancing cooperation and information sharing, the 2010 Conference on Cyber Conflict has brought together communities of techies, national security thinkers, and lawyers interested in cyber conflicts and other closely related areas. The goal of the conference is to facilitate an open exchange of ideas, inspire cross-disciplinary research and cooperation, and to help solve the multitude of problems concerning conflicts in cyberspace. To support this goal, attendees include academic scholars and professionals in industry and government. ; The presentations are based on peer-reviewed papers or strong professional experience.

Since there are no commonly accepted accounts of cyber wars, and some researchers question the mere existence of cyber warfare, the topic of the conference was broadened to cyber conflicts. The CCD COE wishes the conference to be a forum for free discussion on cyber conflicts and a vehicle to achieve a consensus over fundamental definitions in the long run.

This year's Conference on Cyber Conflict is divided into three tracks – Law & Policy, Concepts & Strategy, and Technical Challenges & Solutions.

The Legal & Policy track continues to look how international legal and policy input materializes at the national level. Current trends in international cyber security legislation and policy will be highlighted, with special attention to cyber security legal and policy documents adopted by major international organizations.

The Concepts & Strategy track leans toward academia and builds on the success of last year's Cyber Warfare conference. This year's track focuses on the manifestation of national power and national security in cyberspace. The problems of modelling and analyzing cyber power and cyber conflict and the implications stemming from anonymous and non-state cyber attack campaigns are also discussed.

The Technical Challenges & Solutions track discusses the nuts and bolts of cyber conflicts and incidents at a detailed technical level. Presentations will explore the use and abuse of computer code, network protocols, and Internet infrastructure, and cover both the offensive and defensive aspects of information and cyber warfare.

These proceedings contain academic, double-blind peer-reviewed papers presented at the CCD COE Conference on Cyber Conflict 2010.

Many thanks to all who were involved in organizing the 2010 Conference on Cyber Conflict, and especially to Ms. Anna-Maria Talihärm, for her enormous effort in ensuring order among the vast number of parallel actions and persons involved.

Christian Czosseck
CCD COE
Tallinn, Estonia
June 1st, 2010

TABLE OF CONTENTS

ABOUT THE COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

The Cooperative Cyber Defence Centre of Excellence (CCD COE) is one of NATO's Centres of Excellence, located in Tallinn, Estonia.

Its mission is to enhance the capability, cooperation and information sharing among NATO, Allied nations and Partners in cyber defence by virtue of education, research and development, lessons learned and consultation.

The CCD COE was formally established on the 14th of May, 2008, and accredited by NATO on the 28th of October in the same year. Its primary goal is to enhance NATO's cyber defence capability. The Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic and Spain as Sponsoring Nations. These nations send national cyber experts to Tallinn to cooperatively work on selected topics in the cyber security field.

Despite its status as an International Military Organization, and NATO and NATO nations being the main addressees of the Centre's products and services, the CCD COE does not fall under the NATO command structure. The Centre is however an active member of the cyber defence community in NATO by providing consultation and assistance where needed.

Annually, the CCD COE Sponsoring Nations approve the Centre's Program of Work. First priority is given to requests from NATO and the Sponsoring Nations. The Centre focuses on providing independent research, recommendations, and consultation. Furthermore it organizes or supports training, exercises and conferences.

In addition to requests from Allied nations and partners, the Centre also conducts cooperation with the private sector and various academic institutions.

ABOUT THE CONFERENCE PRESENTATIONS

This year, about 1/3 of the presenters wrote an academic paper, which are included in these proceedings. Their submissions have passed a strong double-blind peer review process and have been approved by an international Program Committee.

PROGRAM COMMITTEE
Chair: Col. **Ilmar Tamm**, Director CCD COE

And the honoured members of the committee:

LAW & POLICY TRACK:
Ms. **Eneken Tikk** (Track Chair),
Dr. **Thomas Wingfield**,
Dr. **Julie Ryan**,

CONCEPTS & STRATEGY TRACK:
Mr. **Rain Ottis** (Track Chair),
Dr. **Irwing Lachow**,
Dr. **Michael R. Grimaila**,

TECHNICAL CHALLENGES & SOLUTIONS TRACK:
Lt.Col. **Marco De Falco** (Track Chair),
Dr. **Enn Tougu**,
Dr. **Gabriel Jakobson**.

The Program Committee ensured high academic standards and originality of the papers, and accepted 13 out of 45 submissions for the proceedings.

They were supported by an international group of reviewers. The Program Committee and the CCD COE want to thank the following reviewers for their review efforts and constructive remarks, they provided:

Prof. **Marta Beltrán**, Rey Juan Carlos University, Spain
Prof. **Jon Bing**, Norwegian Research Center for Computers and Law, Norway
Dr. **Catharina Candolin**, Finnish Defence Forces, Finland
Prof **Antanas Cenys**, Vilnius Gedim inas Technical University (VGTU), Lithuania
Lt.Col. **Antonio Colella**, Italian Army
Dr. **G.W. Ray Davidson**, Purdue University Calumet, USA

Prof. **Dorothy E. Denning**, Naval Postgraduate School, USA
Assoc. Prof. **Ronald C. Dodge**, United States Military Academy, USA
Dr. **Robert Fanelli**, United States Military Academy, USA
Mr. **Kenneth Geers**, Cooperative Cyber Defence Centre of Excellence, Tallinn
Capt. (Eng.) **Antonino de Gregorio**, Italian Air Force
Prof. **Eric T. Jensen**, Fordham University School of Law, USA
Dr. **Marieke Klaver**, TNO Defence, Security and Safety, The Netherlands
Dr. **Pavel Laskov**, University of Tübingen, Germany
Asst. Prof. **Sean Lawson**, University of Utah, USA
Asst. Prof. **Scott Lathrop**, United States Military Academy, USA
Mr. **Felix Leder**, University of Bonn, Germany
Dr. **Corrado Leita**, Symantec Research Labs Europe
Assoc. Prof. **Samuel Liles**, Purdue University Calumet, USA
Mr. **Juan Lopez Jr,** Center for Cyberspace Research at the Air Force Institute of Technology, USA
Mr. **Eric Luiijf**, TNO Defence, Security and Safety, The Netherlands
Prof. **Paulo Sérgio T. de Magalhães**, Universidade Católica Portuguesa, Portugal
Prof. **Peter Martini**, University of Bonn, Germany
Maj. **Andrea Martorelli**, Italian Air Force Staff
Capt. (Eng.) **Giuseppe Mendico**, Italian Air Force
Dr. **Jose Nazario**, Arbor Networks
Dir. **Lars D. Nicander**, Center for Asymmetric Threat Studies, Swedish National Defence College, Sweden
Dr. **Ants Nõmper**, Raidla Lejins & Norcous & Tartu University, Estonia
Prof. **Louis-Francois Pau**, Copenhagen Business School, Denmark
Mr. **Jaan Priisalu**, Swedbank, Estonia
Mr. **Tim Stevens**, King's College, United Kingdom
Dr. **Josef Vyskoc**, VaF &Bratislava School of Law, Slovak Republic
Dr. **Risto Vaarandi**, Cooperative Cyber Defence Centre of Excellence, Tallinn
Prof. **Peter Wahlgren**, Stockholm University, Schweden
Mr. **Tillmann Werner**, University of Bonn, Germany
Asst. Prof. **Stefano Zanero**, Milano Technical University, Italy

Further Conference Organizers:

Local Arrangements: **Raivo Terve & Leelet Nellis**
Public Relations: **Liisa Tallinn**
Sponsorship: **Kenneth Geers**

CCD COE'S CONFERENCE ON CYBER CONFLICTS 2010 SUPPORTERS & SPONSORS

European Union
Regional Development Fund

Investing in your future

BreakingPoint™
Find it before they do.™

Microsoft®

NETWITNESS

skype™

BIOGRAPHIES OF CONTRIBUTORS

AUTHORS

Alexei Konovalov is a PhD student of Research Laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science. He is graduated from Saint-Petersburg Electrotechnical University in 2003. His research interests include security modeling and simulation and software development.

Andrey Shorov is a PhD student of Research Laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science. He is graduated from St. Petersburg State University of Engineering and Economics in 2008. His research interests include security modeling and simulation and software development.

Antoine Lemay is a PhD candidate in computer engineering at the École Polytechnique de Montréal. His research interests are computer security and critical infrastructure protection. In particular, he is looking for ways to protect the critical infrastructure from highly motivated attackers such as foreign states engaging in cyberwarfare.

Daniel Kuehl is the Director of the Information Operations Concentration, a specialized curriculum on national security in the information age offered at the National Defense University. His courses concentrate on such issues as the information component of national power, information operations, cyberspace, and strategic communication. Dr. Kuehl retired as a Lieutenant Colonel in 1994 after nearly 22 years active duty in the USAF. He holds a PhD in History from Duke University and is on the editorial boards of Joint Force Quarterly, Journal of Information Warfare, The Information Operations Journal, and the Journal of Military Studies (in Finland). Dr. Kuehl is a member of the Public Diplomacy Council, the Information Operations Institute, and the Cyber Conflict Studies Association. He was a member of the Defense Science Board team that wrote the 2004 report on Strategic Communication, and is a member of the Public Diplomacy Council.

Forrest Hare is a Lieutenant Colonel in the United States assigned to the Office of the Secretary of Defence, United States Defence Department. In his most recent assignment, he was responsible for developing the United States Air Force's cyberspace strategy as part of Military Strategy for Cyberspace Operations. In addition, he has served in numerous information operations positions world-wide.

Lt Col hare is currently a PhD candidate enrolled at the George Mason School of Public Policy studying national security policy for cyberspace. He has instructed Economics and Geography at the United States Air Force Academy and the University of Maryland Asian Division. He received his Bachelor of Science degree from the United States Air Force Academy, and a Master of Arts from the University of Illinois. He also conducted post-graduate studies at the University of Fribourg, Switzerland, under a Swiss University Grant.

Gunnar Piho is a PhD student at Tallinn University of Technology and a research officer in bioinformatics, at the University of Leeds. He has worked for more than 20 years as a software developer. His main research focus is archetypes and archetype patterns based engineering techniques of domains, requirements and software. His research area is the requirements of clinical laboratory software.

Igor Kotenko is a professor of computer science and Head of Research Laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science. He obtained the Ph.D. degree in 1990 and the National degree of Doctor of Engineering Science in 1999. He is the author of more than 120 refereed publications, including 12 study books and monographs. His research interests include network security, security modeling and simulation, artificial intelligence, multi-agent systems, data mining and telecommunication systems.

Innar Liiv is an Associate Professor in the Department of Informatics at Tallinn University of Technology, Estonia. His research interests include philosophy of artificial intelligence, data mining, predictive and visual analytics, prediction models (churn, fraud, lifetime value), business intelligence in logistics, econometrics, visualization, social network analysis and optimization problems in general. Innar Liiv received a PhD in Computer Science from Tallinn University of the Technology.

Jaak Tepandi is a professor in the Department of Informatics at Tallinn University of Technology, Estonia. His research interests include computer systems security, interoperability, and audit. Jaak Tepandi received a PhD in computer science from the Estonian Academy of Sciences. He is a member of the IEEE Computer Society and the ACM.

José M. Fernandez is a professor at the Computer & Software Engineering department at the École Polytechnique de Montréal. He holds a Ph.D. from the Université de Montréal, a M.Sc.A from the University of Toronto, and B.Sc. in Mathematics and in Computer Engineering from the Massachusetts Institute of Technology. His current research interests include experimental computer security, cyber warfare doctrine and semantic security.

Jüri Kivimaa is currently scientist at the Cooperative Cyber Defence Centre of Excellence. Before this he worked for many years for government and private sector, like the Union Bank of Estonia as a IT security expert. Jüri graduate at the Tallinn University of Technology and holds a diplomaed engineer in electronics. Currently he is PhD student at the Estonian Business School. His research interest lays in costs and efficiency optimizing modeling for Cyber Security.

Peeter Lorents is heading the Research and Development Branch in the Cooperative Cyber Defence Centre of Excellence and in addition holds the position as a full professor at the Estonian Business School, teaching there and at the IT-College in Tallinn. He got his PhD in mathematical logic and theory of algorithm from St Peterburg (f.k.a. Leningrad) State University. Peeter has been elected twice to the Estonian Parliament (Riigikogu), and acted as chairman of the Defense Committee of the Parliament of the Republic of Estonia.

Rain Ottis is a scientist at the Cooperative Cyber Defence Centre of Excellence. He previously served as a communications officer in the Estonian Defence Forces, focusing primarily on cyber defence training and awareness issues. He is a graduate of the United States Military Academy (BS, Computer Science) and Tallinn University of Technology (MSc, Informatics). He continues his studies at a PhD program in Tallinn University of Technology, where he focuses on politically motivated cyber attack campaigns by non-state actors. His research interests include cyber conflict and politically motivated cyber attacks.

Ryan T. Kaminski is a Masters of International Affairs candidate at Columbia University's School of International and Public Affairs concentrating in international security policy. He received his BA from the University of Chicago in June 2008. His primary research interests include US Foreign and national security policy as well as the role of international institutions in global security. Ryan is currently a US Department of Homeland Security Graduate Fellow and was a 2008-2009 Fulbright Fellow in Hong Kong.

Samuel Liles as an associate professor of computer information technology at Purdue University Calumet researching cyber warfare and cyber terrorism. His research agenda follows the spectrum of information operations and how cyber warfare realistically impacts the kinetic effects of conflict.

Scott J. Shackelford holds a Doctor of Jurisprudence from Stanford Law School, and is currently a Ph.D. candidate in international relations at the University of Cambridge. His forthcoming book, The New Cyberwarfare: Countering Cyber Attacks in International Law, Business and Relations, is being published by Cambridge University Press in 2011.

Scott Knight is an Associate Professor in the Department of Electrical and Computer Engineering at the Royal Military College of Canada. He was appointed to the academic faculty at RMC in 2000 on retirement from 21 years of service in the Canadian Air Force. At RMC he founded the Computer Security Laboratory, and continues to lead this research group. This research group has a close working relationship with the Canadian Forces Information Operations Group and focuses on computer network defence and support to information operations.

Stuart H. Starr is a Distinguished Research Fellow at the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU). Concurrently, he serves as President, Barcroft Research Institute (BRI). Prior to founding BRI, Dr. Starr was Director of Plans, The MITRE Corporation; Assistant Vice President for C3I Systems, M/A-COM Government Systems (currently a unit of SAIC); Director of Long Range Planning and Systems Evaluation, OASD(C3I), Office of the Secretary of Defense (where he was member of the Senior Executive Service); and Senior Project Leader, Institute for Defense Analyses. Dr. Starr received a PhD and MS in Electrical Engineering from the University of Illinois, and a BSEE from Columbia University. He has received the Clayton Thomas medal (2004) and the Vance Wanner medal (2009) from the Military Operations Research Society (MORS) for lifetime accomplishments in operations analysis.

Terry Pudas is a Senior Research Fellow at the Center for Technology and National Security Policy at the National Defense University. His work is primarily focused on transformation and related national security issues. Prior to joining the Center, he served as the Deputy Assistant Secretary of Defense (acting), Forces Transformation and Resources in the office of the Under Secretary of Defense for Policy. In September of 2001 he was appointed as the Deputy Director of the newly created Secretary of Defense Force Transformation Office. He served as the Acting Director from January 2005 to October 2006. His primary role was to serve as advocate, focal point, and catalyst for the Department of Defense transformation efforts.

Toomas Kirt is a post-doc researcher at University of Tartu. In 2007 he received a PhD from Tallinn University of Technology. Research interests include artificial intelligence, neural networks, pattern recognition and self-organization.

Vincent Joubert holds a Master in International Relations, Security & Defense from Jean Moulin Lyon 3 University in France and is currently finishing his second Master degree in International Expertise at the same University. He just completed an internship at Raoul Dandurand Chair, UQAM in Montreal where he worked on the security discourses and policy adaptations regarding cyberspace. His research interests lie in cyber security and its consequences on international relations.

PROGRAM COMMITTEE MEMBERS

Ilmar Tamm, Colonel in the Estonian Defense Forces, is currently the Director of the Centre of Excellence of the Cooperative Cyber Defence. After graduating from Finnish National Defence University, he hold various signal and IT related military assignments, including Chief of Communication and Information Systems Department (J6) in the General Staff of the Estonian Defence Forces and 3 years at the Allied Land Component Command Headquarters Heidelberg, Germany as G6 Current Operations and Exercises Section Head. During this assignment, he was deployed to Afghanistan, HQ ISAF in Kabul, as Chief Operations CJ6 Joint CIS Control Centre (JCCC).

Eneken Tikk holds a Magister Juris degree from the University of Tartu and is currently pursuing a PhD degree. After working many years for both government and private sector enterprises, advising on information law, she joined the Cooperative Cyber Defence Centre of Excellence activation team, later becoming the head of the Centre's Legal Task Team. Eneken headed the Cyber Defence Legal Expert Team involved in the drafting of Estonian Cyber Security Strategy; she is also a frequent lecturer on information technology and information law in Estonian universities and author of an infromation law textbook. Currently she is acting Legal and Policy Branch Chief at CCD COE. Her areas of research interest include information technology and cyber security law, as well as legal policy.

Thomas Wingfield is the Professor of International Law at the George C. Marshall European Center for Security Studies. He holds a Doctor of Laws (J.D.) and a Master of Laws (LL.M., International and Comparative Law) from the Georgetown University Law Center, and is completing his Doctor of Juridical Science (S.J.D., National Security Law) at the Law School of the University of Virginia. Professor Wingfield is a former naval officer and has worked in the private sector, think tanks, and academia, most recently at the US Army's Command and General Staff College. He is a former chair of the American Bar Association's Committee on International Criminal Law, and the author of the legal text "The Law of Information Conflict: National Security Law in Cyberspace." Professor Wingfield has just returned from a deployment in Afghanistan as the Rule of Law Advisor to General McChrystal's Counterinsurgency Advisory and Assistance Team. His wife Kim is a Professor of Renaissance Art History and their son John Percival (age 2) has yet to choose a professional track.

Julie J.C.H. Ryan holds a BS from the US Air Force Academy, an MLS from Eastern Michigan University, and a D.Sc. from The George Washington University. After having worked many years in both government and industry, she made the change to academia and is currently an Associate Professor of Engineering Management and Systems Engineering at GWU in Washington, DC. Her areas of research interest

include information security, information warfare, and risk management.

Rain Ottis is a scientist at the Cooperative Cyber Defence Centre of Excellence. He previously served as a communications officer in the Estonian Defence Forces, focusing primarily on cyber defence training and awareness issues. He is a graduate of the United States Military Academy (BS, Computer Science) and Tallinn University of Technology (MSc, Informatics). He continues his studies at a PhD program in Tallinn University of Technology, where he focuses on politically motivated cyber attack campaigns by non-state actors. His research interests include cyber conflict and politically motivated cyber attacks.

Irving Lachow is a Professor at the National Defense University's iCollege and Director of Cyber Programs for the Special Capabilities Office in OSD. Dr. Lachow has extensive experience in both information technology and national security. He has worked for Booz Allen Hamilton, the RAND Corporation, and the Office of Deputy Under Secretary of Defense (Advanced Systems & Concepts). Dr. Lachow received his Ph.D. in Engineering & Public Policy from Carnegie Mellon University. He earned an A.B. in Political Science and a B.S. in Physics from Stanford University.

Michael R. Grimaila is an associate professor in the Systems and Engineering Management department and a member of the Center for Cyberspace Research at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio USA. He is a Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), and holds National Security Agency (NSA) IAM/IEM certifications. He teaches and conducts research in the areas of data communications, database, information assurance, information operations, and information warfare. Dr. Grimaila serves as an Editorial Board member of the Information System Security Association (ISSA) Journal and consults for a number of Department of Defense organizations. He is a member of the ACM, IRMA, ISACA, ISC2, ISSA, ISSEA, and is a senior member of the IEEE. Michael holds a BS, Electrical Engineering; MS, Electrical Engineering; and PhD, Computer Engineering, all from Texas A&M University, College Station, Texas USA.

Marco De Falco, Lt.Col. in the Italian Air Force, is specialized in network management and security. After different military assignments in Italy, latest being in charge of the Italian Air Force WAN management and security unit including the Air Force CERT, he joined the Cooperative Cyber Defence Centre of Excellence as scientist and Italian National Military Representation. Lt. Col. De Falco holds a B.Sc. in Computer Science and a M.Sc. in System Analysis.

Enn Tyugu has a Dr. Sci. degree in computer science from St. Petersburg Electrotechnical Institute. He has served as a professor of computer science at the Tallinn University of Technology and at the Royal Institute of Technology (KTH) in Stock-

holm. Furthermore he is member of the Estonian Academy of Sciences, of IEEE Computer Society and of the Estonian IT Society. His present position is leading research scientist at the Institute of Cybernetics of the Tallinn University of Technology and scientist at the Cooperative Cyber Defense Center of Excellence. His research interests are in intelligent software and cyber-security.

Dr. Gabriel Jakobson is the Chief Scientist at Altusys Corp., Princeton, NJ USA, a consulting firm specializing in intelligent Situation Management technologies for defence and cyber security applications. During his 20 years tenure at Verizon (formerly GTE) Laboratories he lead projects in advanced databases, expert systems, artificial intelligence, and network management. Dr. Jakobson has authored over 100 technical publications, holds 4 US patents on event correlation and has 4 US patents pending on situation management. He received PhD degree in Computer Science from the Institute of Cybernetics, Estonia. Dr. Jakobson holds an honorary degree of Doctor Honorius Causa from the Tallinn Technical University, and is Distinguished IEEE ComSoc Lecturer. Dr. Jakobson is the chair of the IEEE ComSoc Sub-Committee on Situation Management.

EDITORS

Christian Czosseck is Scientist at the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Being a soldier in the German Armed Forces (Bundeswehr) for more than 12 years he held several Information Assurance positions in the German military. Christian graduated first in his class in computer science at the Universität der Bundeswehr in Munich, and is currently PhD student at the Estonian Busines School in Tallinn.

Karlis Podins has a Bachelor's and Master's degrees with distinction in computer science from University of Latvia. He has joined the Cooperative Cyber Defence Centre of Excellence research&development branch after being a research assistant in Institue of Computer Science, University of Latvia.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

AGENT-BASED MODELING AND SIMULATION OF BOTNETS AND BOTNET DEFENSE

Igor Kotenko, Alexey Konovalov, and Andrey Shorov[1]

Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, St. Petersburg, Russia

Abstract: Nowadays we are witnesses of the rapid spread of botnets across the Internet and using them for different cyber attacks against our systems. Botnets join a huge number of compromised computers in the Internet and allow using these computers for performing vulnerability scans, distributing denial-of-service (DDoS) attacks and sending enormous amounts of spam emails. It is a very complex task to detect such botnets and protect against their attacks. The paper considers the approach to the investigation of botnets and botnet defense mechanisms. The approach is based on the agent-based simulation of cyber attacks and cyber defense mechanisms, which combines discrete-event simulation, multi-agent approach and packet-level simulation of network protocols. The various methods of botnet attacks and counteraction against botnet DDoS attacks are explored by representing botnets and botnet defense components as agent teams using the software simulation environment under development. Agents are supposed to collect information from various sources, use different knowledge, forecast the intentions and actions of other agents, try to deceive the agents of competing team, react to actions of other agents. The teams of defense agents are able to cooperate as the defense system components of different organizations and Internet service providers (ISPs). The paper outlines the common framework and implementation peculiarities of the simulation environment as well as the experiments aimed on the investigation of botnets and botnet DDoS defense mechanisms.

Keywords: cyber conflicts, cyber defense, botnets, Internet attacks and defense, DDoS, modeling and simulation, packet-based simulation, agent-based systems

1 39, 14th Liniya, SPIIRAS, St. Petersburg, 199178, Russia, Emails: {ivkote, konovalov, ashorov}@comsec.spb.ru.

INTRODUCTION

In April-May 2007, Estonia experienced several weeks of coordinated cyber attacks against its financial and sociopolitical institutions. As many authors declared, in this case Europe experienced its first information war (Blank, 2008). These attacks included huge denial of service attacks inspired by botnets.

A botnet is a computer network that consists of a certain number of hosts, where bots are run. A bot is standalone software. Most often the bot in the botnet is a program that is surreptitiously installed on the victim's computer and allows an attacker to perform some actions using the resources of the infected computer. Today, botnets confidently occupy the leading positions in the list of current threats to the Internet.

With the advent of botnets, malefactors have got access to millions infected computers of users, and the number cyber crimes has increased by hundreds of times. According to the FBI for October, 2009, losses because of botnets have reached about $100 million. Now experts observe the amplification of competition in the market of botnets, for example, at the end of 2009 – the beginning of 2010 a lot of new botnet programs, such as Filon, Clod, Buga, Spy Eye, has appeared (Truhanov, 2010).

The distinctive features of modern botnets as tools for cyber crime are a wide variety of possible targets of attacks, including the theft of personal or any other confidential data (theft of money from electronic invoices, credit card numbers, etc.), spam, forced advertise show, DDoS attacks, use of infected computers in their own purposes, compromise of legitimate users, cyber blackmail, fraud of rating tracking systems (for example, attack ClickFraud). The spectrum of the attacks, implemented by means of botnets, is rather extensive. Botnets are potentially suitable for attacks as in areas directly connected with cyber security, as well as in sphere of social engineering (Colarik, 2006).

Functioning of botnets is characterized by the simultaneous actions of a great number of software agents in the interests of malefactors. In most cases, a malefactor gains complete control over the resources of infected computers and can freely use them in almost any of their own interests. The prominent aspect of botnet use is the orientation of attackers usually on political goals or financial results, and, as a consequence, a high level of attack preparation. It stipulates considerable difficulty in identifying the organizers of botnets and in neutralizing them.

The last years, in particular, in Russia the following tendencies for botnets were observed (Lopuhin&Sachkov 2009):

- Enlargement – small botnets evolved in a larger ones; there was their associa-

tion and escalating of force for the opportunity of more powerful attacks;

- Decentralization – the command and control centers were transferred to the countries of "the third world" and decentralized;
- Occurrence of nonprofessional botnets by using special toolkits for their creation; the special knowledge for creation and management of such botnet is not required;
- Professional botnets began to use advanced technologies for command, control, communication, intelligence and maintenance of anonymity. In particular, some botnets began to use portknocking authentication technology (www.portknocking.org) etc.

All this emphasizes the urgency of research on protection against botnets. One of the major tasks of such research is an investigative modeling and simulation of botnets and defense mechanisms against them. The purpose of the research is the development of effective methods and means for botnet counteraction.

The paper considers *an approach to investigation of botnets and botnet defense mechanisms*. The approach is *based on the agent-based simulation of cyber attacks and cyber defense mechanisms, which combines discrete-event simulation, multi-agent approach and packet-level simulation of network protocols*. Initially this approach was suggested for network attack and defense simulation in (Kotenko&Ulanov 2006 a,b, 2007, 2008). In the present paper as against other works of authors the various methods of botnet attacks and counteraction against botnets are explored by representing attack and defense components as agent teams.

The global goal of our research is to *develop the usable common framework and simulation environment (integrated software tool) for analysis of botnets and botnet defense mechanisms*. The paper makes the greatest accent on specifying the scenarios of botnet functioning and defense mechanisms, describing the agent-based simulation environment under development and presenting the results of experiments carried out.

The paper is structured as follows. The first section describes the relevant papers and the features of proposed approach. Second section outlines the architecture and current implementation of agent-based simulation environment. Third section presents the configuration of simulation environment for experiments. Forth section considers the examples of experiments conducted. Conclusion outlines the main results and future work directions.

1. RELATED WORKS AND THE APPROACH TO SIMULATION

Current research on botnets and botnet defense can be considered mainly in two categories – botnet detection/response techniques and botnet measurement (Bailey, et al., 2009, Liu, et al., 2009, Strayer, et al., 2008). Botnet detection can be implemented, for example by detection via bot cooperative behaviors (Gu, et al., 2008a,b, 2007, Karasaridis, et al., 2007, Strayer, et al., 2006), detection by signatures of botnet communication process (Binkley&Singh 2006, Goebel&Holz 2007), and detection and response to attacks (Chen&Song 2005, Mirkovic, et al.,2004, 2005, Xie, et al.,2008). Measurement papers allow understanding the botnet phenomenon and the characteristics of specific types of botnets (Bailey, et al., 2009). Examples of papers on botnet measurement are (Dagon, et al.,2007, Gianvecchio, et al.,2008, Grizzard, et al., 2007, Kanich, et al., 2008, Rajab, et al.,2007, Wang, et al., 2007, Zhu, et al., 2008).

The most dangerous classes of attacks, which are the basic attack means of botnets, are *DDoS attacks* (Mirkovic, et al.,2004). *Traditional defense* from such attacks includes detection and reaction mechanisms. To detect abnormal network characteristics, many methods can be applied (for instance, statistical, cumulative sum, pattern matching, etc). The examples of detection methods are Hop counts Filtering (HCF), Source IP address monitoring (SIPM), Bit per Second (BPS), etc. As a rule, the reaction mechanisms include filtering, congestion control and traceback. As the detection of Botnet DDoS is most accurate, when it is close to the victim hosts, and the separation of legitimate is most successful close to the sources, adequate victim protection against Botnet DDoS to constrain attack traffic can only be achieved by *cooperation of different distributed components* (Mirkovic, et al., 2005). There are a lot of architectures for distributed cooperative defense mechanisms, e.g. Server Roaming, Market-based Service Quality Differentiation (MbSQD) (Mankins, et al., 2001), Transport-aware IP router architecture (tIP) (Wang&Shin 2003), Secure Overlay Services (SOS) (Keromytis, et al., 2003), ACC pushback, COSSACK (Papadopoulus, et al., 2003), Perimeter-based DDoS defense (Chen&Song 2005), DefCOM (Mirkovic, et al., 2005), Gateway-based (Xuan, et al., 2001).

The approach to botnets and botnet defense modeling and simulation, developed in the paper, is based on works in various fields. The basis of the proposed approach is agent-based modeling and simulation. Its essence is in representing the entities of subject area as particular autonomous intelligent agents. A set of intelligent agents, with simple functions, in process of their activities can be self-organized into a system with complex behavior needed for modeling and simulation of botnets and botnet defense.

The variety of frameworks and architectures for multi-agent modeling and simulation of distributed complex systems was developed, e.g. shared plans theory (Grosz&Kraus 1996), joint intentions theory (Cohen&Levesque 1991), hybrid approach (Tambe, 1997), there were implemented various software multi-agent environments (Macal&North 2005, Marietto, et al., 2002). The approaches based on belief-desire-intention (BDI), distributed constraint optimization (DCOP), distributed POMDPs, and auctions or game-theoretic (Tambe, 1997) are emphasized. Different mechanisms for collaborative agent team maintenance are suggested (Kaminka, et al., 2007). The main task of these approaches is *to provide the optimal interaction of heterogeneous components to reach some high level goal*. These methods, models and tools have been applied in different subject domains (Haque, et al., 2005, Jennings 1995, Kaminka&Frenkel 2005, Tambe, 1997).

The property of self-organization of agents into teams makes it appropriate to use them in problems related to cooperative games (Russell&Norvig 2009). Agents can get information about other agents, as well as on the state of environmental factors. Based on these data and on the basis of past experience and their functional role, the agent makes a decision regarding its future behavior. Thus, for effective decision-making, it is required to find an effective way to represent knowledge about the model of the external world inside the agent, using the theory of knowledge representation and the logic of reasoning. Goals may be common to a set of agents. Successful achievement of such objectives requires decision of problems related to cooperation and coordination of agents. Often the objectives for the group of agents are mutually exclusive; therefore, to build effective collective strategies, it is necessary to use the theory of antagonistic games.

The properties of the network environment, which is a space for network device operation, are characterized by high variability. The account of varying properties of the environment in the agent model stipulates the need to its adaptation and learning. Using agents as independent structural units does not exclude the presence of knowledge that is external to the agents and shared by them. Such knowledge can be a repository of collective and multi-level goals, the successful achievement of which requires the use of planning methods.

In the paper, the botnet life cycle and the process of botnet containment by defense mechanisms are simulated. Similarly to botnet structure, the structure of defense mechanisms is implemented by the subnet of defense components (agents). Both subnets are part of the overall computer network imitating the behavior of a certain segment of the Internet.

The paper also presents a model of the computer network topology in the form of a random graph, parameterized by statistical data obtained by measuring the topology of the Internet (Zhou, et al., 2006). Traffic is simulated on the level of individual

network packets, and is implemented by modeling the behavior of network applications. The behavior of network applications has a stochastic nature and is specified by a number of statistical parameters, whose values were derived from the study of network applications. The processes of sending, receiving and passing the network packets on communications channels are imitated through a discrete event simulation system.

The model of botnet, presented in the paper, is based on the results of earlier works conducted by several investigators (Bailey , et al., 2009, Barford&Yegneswaran 2007, Bradley&Harley 2007, Christodeorescu&Rubin 2007, Dungam&Meluick 2008, Mirkovic, et al., 2004, Strayer, et al., 2008). In particular, in some papers the structure of the botnet life cycle, the phases of botnet functioning as well as the technological and organizational aspects of each phase were outlined (Barford&Yegneswaran 2007, Anon. 2007, Mirkovic, et al., 2004).

In this paper, the models of botnets and botnet defense are specified in the form of a common model of counteraction between the two classes of teams – the attack team and the defense team. Each team represents a subset of computer network nodes, identified as agents, and having a common collective goal. Attack team includes agents belonging to the botnet and implementing actions aimed at achieving the collective goal – providing the vital activity of botnets. An example of the collective goal of the attack team is a DDoS attack against some pre-identified resource. Similarly, the defense team is made up of agents, performing the defense functions and having a collective goal to oppose the botnet. It is supposed that the team of botnet agents evolves by generating new instances and types of attacks and attack scenarios to overcome the defense. The team of defense agents adapts to the botnet actions by changing the security policy and forming new instances of defense methods and profiles.

The following main *simulation components* are represented on the basis of this approach: models of agent teams; models of team interactions; interaction environment model.

Models of agent teams are intended to represent the investigated processes. They include particular team ontologies, agent basic functions, agent classes, agent protocols and behavior scenarios. *Team ontologies* are based on the subject domain ontology and include the notions and relations used by agents of this team. The list of *agent basic functions* includes the following functions: initialization; shutdown; access to the agent ontology; management of active agents list; basic work with transport-level modules (connection establishing, message sending, connection closing). The needed *agent classes* are defined for the teams. The amount of agents of predefined classes is set in each team. *Agent interaction protocols* are represented as the sequence of instructions with specific parameters. The type of instruc-

tion defines how to use these parameters. The conditions of protocol initialization provide communication selectivity for agents. Agent interaction protocols are based on the transport layer that is provided by the communication environment. Agent team establishing protocol is the part of procedures for monitoring and recovery of agent functionality. *Scenarios* represent various stages of team actions. Adaptation procedures are implemented in scenarios to act depending on other team actions and environment reaction. Agent team behavior scenarios ensure action consistency maintenance. (Ulanov & Kotenko 2008)

Models of team interactions include the models of antagonistic competing and team cooperation. *Model of antagonistic competing* lies in the basis of competing teams' interaction. This model defines the goals, sub-goals, intentions and actions of competing teams that are aimed on the interaction environment or (and) the opponent team. *Cooperative interaction* happens between teams that pursue the same goal. The proposed model of cooperation is based on the exchange of information between teams. Such exchange is made to raise the effectiveness of reaching the common goal and occurs on several different levels with the use of agents of various classes. For example, in the task of cooperative network defense simulation it is possible to exchange attack signatures, network traffic data, filtering requests, etc.

2. SIMULATION ENVIRONMENT

To implement the proposed approach, a software environment is required, that has a wide range of opportunities to support network simulation. In the first place, we need a possibility to simulate the network systems with arbitrary topology and communication processes between different nodes at the level of discrete events. To simulate real-world communication scenarios, observed in the Internet, we must have the models of protocols and network applications.

The description of individual and group behavior of agents as well as experiment parameters supposes the presence of a high level language to specify such behavior scenarios and parameters.

The authors of the paper are trying to use and develop a multi-level instrumental environment for simulation of network processes. This environment is a software package that includes a discrete event simulator, implemented by low-level language, and a number of components that realize the components of higher levels.

The lower level provides a possibility to simulate the chronologically ordered sequences of events, propagating in network structures. Intermediate levels on the basis of the lower level implement the components related to the specifics of the Internet, including the models of protocols and standard network applications. Inter-

mediate levels are the basis for constructing components of a higher level, such as, for example, the level of intelligent agents. All modules and components of the simulation environment are in conjunction with the I/O subsystem and, thus, through this subsystem can communicate with external data sources and with the system operator. Each level is implemented as a separate function library with a documented interface. Such interface ensures the opportunity to interact with this library from the side of other components.

The architecture of simulation environment consists from four main components (Figure 1).

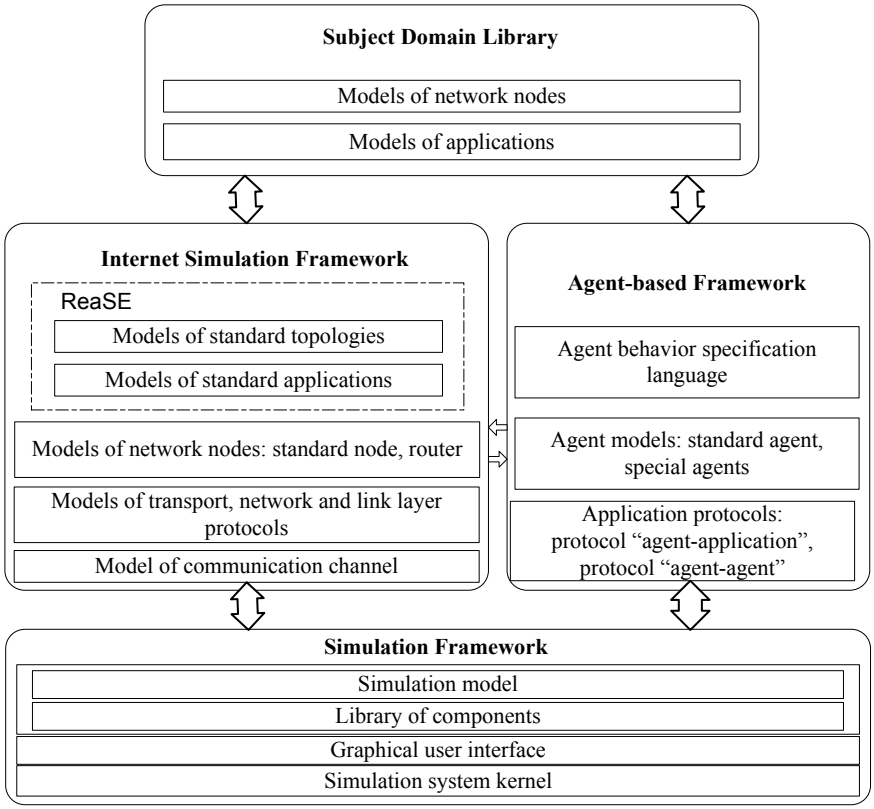

Figure 1. Architecture of simulation environment

Simulation Framework is a discrete event simulation system. It provides tools for modeling chronologically ordered sequences of discrete events. Simulation Framework implements the basic models of random event distributions and the basic mod-

els of queues with priorities and the collection of statistics. The possibilities of basic model data input/output and basic features for processing the results of experiments are provided.

Internet Simulation Framework is a set of modules which allow simulating nodes and protocols of the Internet. It contains the modules that form realistic network topologies, the models of network applications with behavior close to the behavior of real network applications, as well as the models of transport, network and link layer protocols. Thus, this component provides the models of computer network as a network with nodes that include a stack of TCP/IP-protocols. Each protocol is implemented as an independent module. Internet Simulation Framework also contains modules for automatic construction of standard networks based on the set of defined parameters and their automatic configuration. In current version this component uses the library ReaSE (Gamer&Scharf 2008).

Representation of network elements as intelligent agents is realized by using *Agent-based Framework*. This component is a library of modules that specify intelligent agents and common scripts of their behavior, implemented in the form of models of services and applications embedded in the models of network nodes. The component also contains the models of application layer protocols, which provide communication between agents and interaction of agents with application models. In addition, the component includes a high-level language interpreter to manage agents and a transmitting module, which converts the commands of the language into the sequence of intelligent agent actions.

Subject Domain Library is a library, which serves to simulate the processes of the subject area. It includes modules that complement the functionality of IP node, including filter tables, packet analyzers, models of legitimate users, etc.

Using several different components, such as the simulator OMNeT++ (www.omnetpp.org), the libraries INET Framework and ReaSE, and our own software components (Kotenko&Ulanov 2006a,b, 2007), the proposed architecture has been implemented for agent-based simulation of botnets and defense mechanisms against them. Models of agents, implemented in Agent-based Framework, include an agent "legitimate client", an agent "legitimate server", attack agents and defense agents. Subject Domain Library contains various models of nodes, for example, attacker, firewall, etc., as well as application models (mechanisms for implementation of attacks and protection, packet sniffers, filter tables).

OMNeT++ is a discrete event simulation system. In the proposed architecture, it is a lower level component. OMNeT++ provides message exchange between the components simulated, experiment visualization, interaction with the user, and debugging the states of objects and sequences of model events. In addition, OMNeT++ provides

a special language to describe connections between components simulated, thus describing the network topology, and allows specifying the experiment parameters. The structure of individual participants, involved in message exchange, is described as C++ classes; the logic of message processing by specific actors is determined by algorithms implemented in C++ class methods. Using the high-level language to specify the static relations between components and the environment parameters allows achieving high flexibility in configuring simulated components, because it does not require translating configuration scripts into binary code. On the other hand, the usage of C++ language for message processing is characterized by low overhead, because the handler code is compiled into a high-performance machine code. Thus, an approach, based on combining the low and high level languages, provides a high performance with a sufficiently flexible configuration mechanism that may be important when conducting multiple experiments.

The main window of OMNET++ graphical development environment (for version 4.0) is shown in Figure 2.

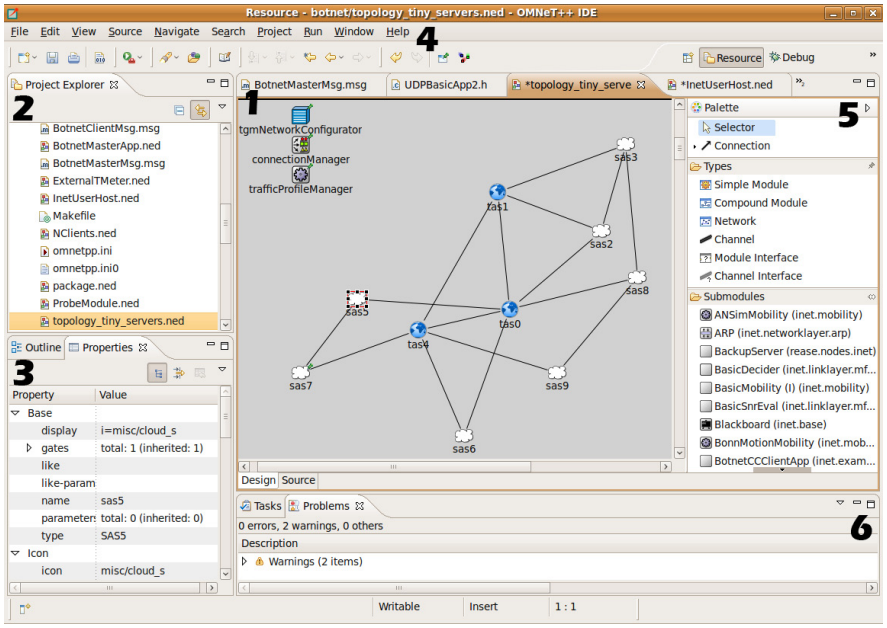

Figure 2. Main window of OMNET++ 4.0 development environment

The development environment window is divided into several zones, which contain a variety of visual tools (sub windows). The main simulation window is marked with 1. It contains the structure of the current component or the view of the whole net-

work. In the upper left corner (2) there is a list of files included in the current model. Below (3), there is a table of properties of currently active object (in the figure it is an object with the name sas5), which is highlighted with a frame on the main window.

Also there is a palette of components (5), available for insertion into the current model, and a console with various information to assemble the model (6). The main menu and toolbar are situated at the top of the development environment. Objects, involved in simulation, are represented by appropriate images with the specified object names. Connections between objects are shown by solid lines.

Figure 2 shows the objects that have connections with other objects and the objects without connections. Unconnected objects are not involved in message exchange and, as a rule, perform various service functions, such as, for example, the configuration of other objects or collecting the statistics.

An example of the model representation in experiments is shown in Figure 3.

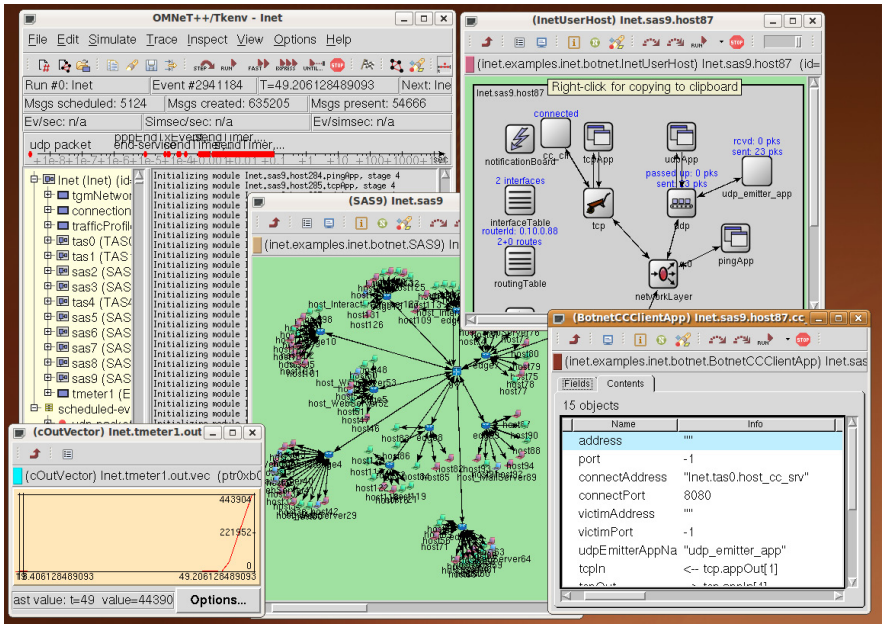

Figure 3. Representation of the model in experiments

In the upper left corner you can see the main panel that displays the components included in the model and control elements that allow the user to interact with them. In addition, the main panel consists of the model time control elements, which allow executing the model step by step or in maximum fast mode. There are also the con-

trol elements to perform an efficient search for the entity of interest and subsequent editing of its condition.

Figure 3 shows a fragment of the simulated network, where the router models are shown as cylinders with arrows, and the host models are in the form of computers having different colors.

Color displays the status of nodes in the botnet. Green represents the nodes that are part of botnet and have a connection to the command center, red – the nodes which have received the command to attack the target. Nodes that are not included in the botnet do not have a color tint.

As an example, Figure 3 also shows the window of a host representation (top right), the window for editing the parameters of the object "bot-client" (bottom right), and the window of current experimental results (bottom left), showing in graphical form the value of one of the investigated parameters.

3. IMPLEMENTATION CONFIGURATION

3.1 NETWORK TOPOLOGY

The network topology is simulated on *two levels of detail*.

On the first level, the network topology on the autonomous system (AS) level is simulated. A number of authors recommend using the PFP (Positive Feedback Preference) method (Zhou, et al., 2006) to simulate the Internet on the autonomous system level. This method allows the most plausible representation of statistical properties of the Internet topology segments. In the paper we describe the experiments in which a network consisting of 5-10 autonomous systems (AS-level topology) is simulated. We generate a graph of autonomous system level with the following parameters: Transit Node Threshold = 10, P = 0.4, Delta = 0.04 (Zhou, et al., 2006). Connections of transit AS are implemented through the communication channel with the bandwidth dr = 10000 Mbit/seconds and the delay d=1 microseconds. Connections of other AS are implemented with dr = 5000 Mbit/seconds and d = 1 microseconds.

On the second level of simulation, for each autonomous system the internal topology (Router-level topology) is simulated. In the paper we use so called HOT (Heuristically Optimal Topology) model (Li, et al., 2004) with the following parameters: Min nodes = 20, Max nodes = 25, Core ratio = 0.05, Core cross link ratio = 0.2, Min hosts per edge = 10, Max hosts per edge = 20 (Li, et al., 2004). Each autonomous system includes approximately 300 end-nodes (Figure 4). The equipment of nodes has the

types “router” or “host’. The equipment “router” has only one functional role – “router”. The equipment “host” is represented by the following set of functional roles: web server, web client, mail server, server of multimedia content, “command center” server, “vulnerable service” (potential “zombie” machine), “master”, IP-filter. At each node the model of standard protocol stack is installed. It includes the protocols PPP, LCP, IP, TCP, ICMP, ARP, UDP. Also, depending on the functional role, the models of network applications are installed. They implement application-level protocols. For each protocol, the appropriate adjustment of its parameters is fulfilled. For example, for IP protocol the corresponding adjustment of routing tables is carried out in accordance with the principle of minimizing the number of intermediate nodes on the route of IP-packet.

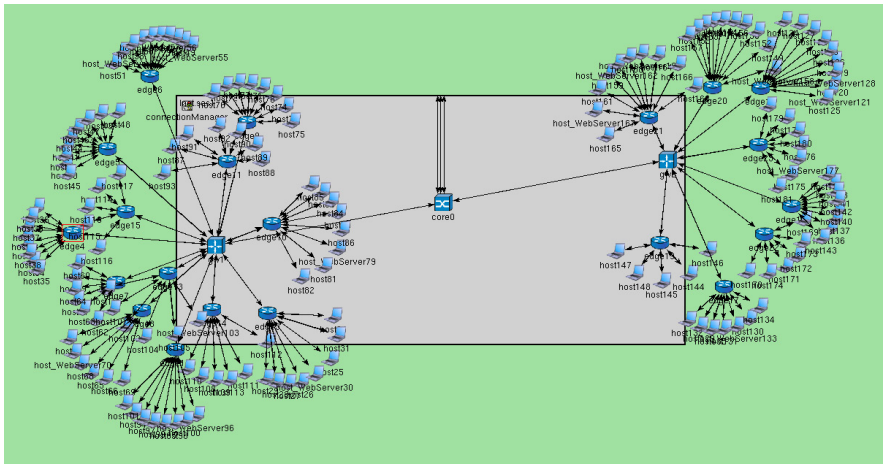

Figure 4. Example of an autonomous system representation

3.2 ATTACK TEAM CONFIGURATION

Attack teams include the following types of nodes: “master”, “command center”, “target”, “zombies”. Node “master”, by sending different commands, sets the goals of the botnet and controls the behavior of the network at the highest level. Node “command center” carries out the delivery of commands received from the “master” to nodes “zombies”. Nodes “zombie”, receiving the commands from the “command center”, immediately carry out actions under the orders of the “master”. In experiments we use a single node “master”, one or several nodes “command center” and a set of nodes with vulnerable software, which can potentially turn into “zombie” machines.

3.3 CONFIGURATION OF LEGITIMATE HOSTS

To generate a legitimate traffic, the set of nodes "server" (in the amount of 10% of the total number of nodes) is determined. The nodes "servers", in response to a request from the nodes "clients", generate the traffic statistically similar to traffic of standard web server (Gamer&Scharf 2008). Vulnerable hosts are determined randomly. They represent about 40% of the total number of nodes. One of examples of a vulnerable service is based on UDP protocol and uses port 80.

3.4 DEFENSE TEAM CONFIGURATION

Defense teams are represented by the following common classes of agents: information processing ("sampler"); attack detection ("detector"); filtering ("filter"); investigation ("investigator"); rate limitation ("limiter"). Samplers collect and process network data for anomaly and misuse detection. Detector coordinates the team, correlates data from samplers, and detects attacks. Filters are responsible for traffic filtering using the rules provided by detector. Investigator tries to defeat attack agents. Limiter is intended to implement cooperative DDoS defense. Its local goal is to limit the traffic according to the team goal. It lowers the traffic to the attack target and allows other agents to counteract the attack more efficiently. (Kotenko & Ulanov 2008)

In experiments, the method of Source IP address monitoring (SIPM) is used as the defense mechanism. It is based on the assumption that during DDoS attacks in the passing traffic, the number of new addresses used for connection with the attacked resource grows quickly.

The module, which implements the defense mechanism, may be in one of two modes: training or working (i.e. anomaly detection and traffic filtering).

In the training mode, the module intercepts the traffic and determines the number of different IP-addresses involved in the communication for a certain time period (parameter tshift). In the experiments the value of tshift is 2 seconds. The data obtained in the training mode are taken as typical traffic values in the node and then are used in the process of anomaly detection.

In the working mode, the module calculates the same parameters and compares them with typical values. When a significant excess of observed nominal values is observed, the protection module generates an anomaly detection signal and provides selective filtering of packets with new IP addresses.

3.5 REALIZATION OF SCENARIOS

To perform the experiments we have realized several scenarios of botnet functioning (including scenarios of botnet propagation, botnet management and attack realization), botnet containment and attack counteraction, and network legitimate activity.

Scenarios of botnet propagation involve scenarios of looking for new nodes suitable for compromise, their identification, subsequent compromise, and connecting the infected nodes to the botnet.

Scenario of botnet propagation used in the experiments is based on the model of a network worm spreading through the exploitation of the vulnerability of network services. After activation of a vulnerable service, the computer is considered infected. An example of a scenario is illustrated in Figure 5. After infection, the infected computer icon turns yellow.

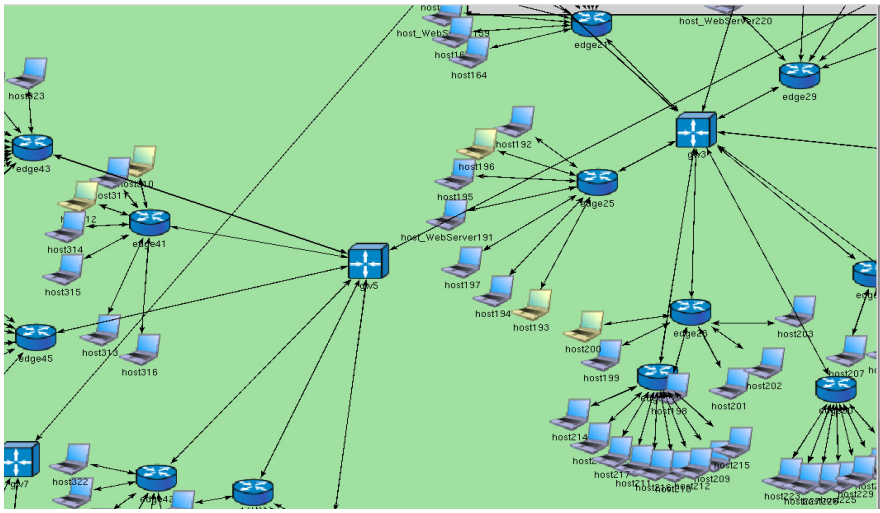

Figure 5. Infected computers

Scenario of connecting the infected nodes to botnet is specified by the procedure of sending the message about the new node status to the server "command center" and then pending the receipt of commands from the server.

One of the examples of implemented *scenarios of botnet attack realization* is an attack "UDP Flood", directed to some node (subnet), the IP-address of which is specified in the attack start command.

We implemented several *scenarios of botnet containment and attack counteraction*,

directed on protection against DDoS attacks: without cooperation; DefCOM-based; COSSACK-based and full cooperation.

In defense scenario *without cooperation* only one defense agent team is used. This team is represented by the following common classes of agents: "sampler", "detector", "filter", "investigator", and "limiter".

In other defense scenarios we use several cooperating defense agent teams which protect different segments of the computer network.

The following agent classes are proposed to introduce in compliance with *DefCOM* architecture (Mirkovic, et al., 2005): "Alert generator" agent is based on a "detector" agent. It gathers traffic data from "sampler", detects the IP-addresses of hosts that generate the greatest traffic. If it exceeds the given threshold, the alert is generated. Agent "Rate limiter" is based on a "limiter" agent. It can drop the packets destined to the attack target providing some volume of traffic. Agent "Classifier" is based on a "filter" agent that receives filtering data from the detector. This agent is able to filter the disclosed attack packets. It also marks the legitimate packets to let "limiter" pass them. When "Alert generator" detects the attack, it sends the attack messages to other agents. Then "Rate limiter" agents start to limit the traffic destined to the attack target. "Classifier" agents start to classify and drop the attack packets and to mark legitimate packets.

COSSACK architecture (Papadopoulus, et al., 2003) consists of the following agent classes: "snort" prepares the statistics on the transmitted packets for different traffic flows; the flows are grouped by the address prefix. If one of the flows exceeds the given threshold, then its signature is transmitted to "watchdog"; "watchdog" receives traffic data from "snort" and applies the filtering rules on the routers. Agent "snort" is based on an agent "sampler". It processes the network packets and creates the model of normal traffic for this network (in the learning mode). Then, in the normal mode, it compares the network traffic with the model and detects the malefactor's IP addresses, which it sends to "watchdog". Agent "watchdog" is based on an agent "detector". It makes the decision about attack due to data from "snort". Agent "filter" is used to simulate the filter on the router. It is deployed on the router and performs traffic filtering using data from "watchdog". "Watchdog"-level cooperation is used to transmit the filtering rules. Cooperation is in the following: when a "watchdog" detects the attack, it composes the attack signature; this "watchdog" sends it to the other known "watchdogs"; "watchdogs" try to trace in their subnets the attack agents that send attack packets; when they detect them, the countermeasures are applied.

Full cooperation architecture stipulates for the following classes of defense agents: "samplers", "detectors", "filters", and "investigators". Under full cooperation the team, which network is the attack victim, can receive traffic data from the samplers of

other defense teams and apply the filtering rules on the filters of other teams.

The algorithms of *network legitimate activity scenario* are based on generation of the model traffic with statistical parameters, similar to parameters of a real network traffic (Vishwanath&Vahadat 2006). They are executed by sub-scenario of session creation, using the parameters which depend on the type of generated traffic.

4. EXPERIMENTS

The investigation of attack and defense scenarios has been done on the basis of analysis of two *main classes of parameters*: the amount of incoming attack traffic before and after filter of team which network is the attack victim; false positive and false negative rates of the defense team, which network is the attack victim.

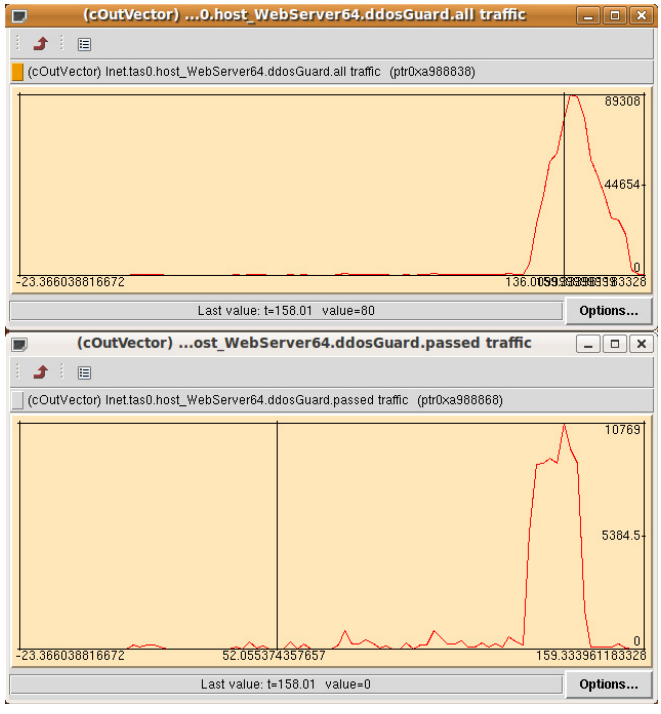

Figure 6. Examples of traffic levels before and after filtering

Under scenarios of botnet containment and attack counteraction, the defense system tries to separate the malicious traffic from the legitimate traffic, and, if possible, to filter out the malicious traffic. The results of the filtering process are estimated by

false positive (FP) and false negative (FN) rates. Examples of traffic levels before and after filtering for one of the experiments for *defense scenario without cooperation* are depicted in Figure 6. The figure shows that the traffic volume after filtering was reduced to nine times. The values of errors of first and second kind are as follows: FN = 0,09, FP = 0,002.

Figure 7 shows the attack traffic inside the attacked subnet for *scenarios of botnet containment and attack counteraction using COSSACK (triangles), DefCOM (dots) and full cooperation scheme (crosses).*

Attack starts at 300 seconds. The random real IP spoofing technique is applied as the most complicated for detection (the addresses for spoofing are taken from the same network).

Attack traffic for COSSACK is measured on the entrance to the defended subnet on the filter. The significant traffic increase is noticed in the beginning of attack. But in the area of 350 seconds the defense system detects the attack. Filtering rules are applied and the traffic inside the subnet is reduced (after 350 seconds). Attack signature is sent to the other defense components. They apply filtering rules in their subnets. The traffic on the entrance to the defended subnet is decreased due to their actions.

The attack traffic inside the attacked subnet for DefCOM is represented with the dots in Figure 7. The traffic was measured at the entrance to the subnet, since the last component in the subnet that changes the traffic is the limiter. It is deployed on the router that has four interfaces and the incoming attack traffic was summarized into one graph. In the area of 350 seconds the defense system detects the attack and traffic is being limited before the defended subnet and being filtered in the source subnets. Rate limiter proceeds to limit the traffic, because of the high attack traffic volume.

The attack traffic inside the attacked subnet for the full cooperation scheme is represented with the crosses in Figure 7. Traffic is measured on the entrance to the defended subnet on the filter. The significant traffic increase is noticed in the beginning of attack. But in the area of 350 seconds the main defense team detects the attack requesting the traffic data not only from its sampler but from the samplers of other teams. Filtering rules are applied and traffic inside the defended subnet is significantly decreased (around 350 seconds). Attack signature is sent to the other cooperating teams. They apply the filtering rules in their subnets. The traffic on the entrance to the defended subnet is decreased due to their actions (after 350 seconds). The system succeeds in decreasing the traffic much more due to permanent attack signatures renewing (400–450 seconds).

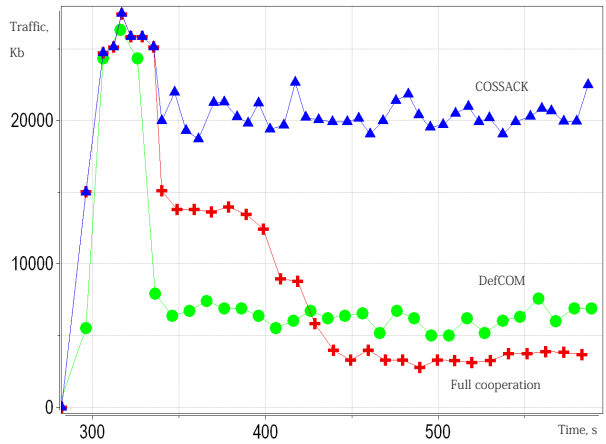

Figure 7. Attack traffic inside the attacked subnet for COSSACK, DefCOM and full cooperation

The experiments implemented demonstrated that full cooperation shows the best results on blocking the attack traffic. It uses several defense teams with cooperation on the level of filters and samplers. Samplers cooperation played the crucial role in defense.

DefCOM comes after full cooperation. Its advantage is in using the rate limiter before the defended network. It allows lowering the traffic during attack and letting the defended system work properly.

COSSACK is the third. It is one of the examples of peer-to-peer defense network. It uses attack signatures transmission between agents to apply the filtering rules near the source. The communication overhead for cooperative defense is restricted by the communication selectivity procedures. The agent protocols can be executed only periodically or in the strict sequence. Therefore their influence on the joint traffic is low.

Different *adaptation schemes of agent teams* were also studied. *Adaptation schemes* operate in the following way. Depending on attack state the defense team adapts the parameters of methods and cooperation reducing the defense cost. The simplest and not the most resource-intensive method is BPS. The defense team starts the defense-implementing BPS. When attack is detected the team continues to use the same method, if it allows the attack to be neutralized. If it fails, then the defense team applies the more complicated SIPM method. If it succeeds to stop the attack, then the defense team returns to BPS. If not – it will additionally use HCF. Conducted experiments showed that one can reach the best attack traffic blocking due to de-

fense teams cooperation.

Since sampler cooperation was the determinative in defense, it can be used without applying full cooperation during which high teams interaction traffic is observed.

Attack team redistributes the attack intensity between daemons and changes the address spoofing technique to minimize the amount of attack packets and reduce the probability of attack agents' exposure by defense agents. At first the team having many daemons distributes the load equal between them and does not use address spoofing (not to draw suspicion upon themselves from firewall in their subnet). If after the defense team actions some of the daemons will be defeated, the attack team will raise the load to the remaining daemons (to save the given attack intensity) and apply the address spoofing technique to avoid detection. If the remaining daemons are not defeated the team will continue the attack in the former mode.

5. CONCLUSION

This paper proposed the approach to simulation of botnets and defense against botnets in the Internet. Botnets and botnet defense is examined by interaction of different agents teams that can be in the relation of antagonistic and non-antagonistic competing or (and) various kinds of cooperation. The main results of the paper consist in specification of formal framework for botnet analysis and implementing the software simulation tool for packet-level agent based simulation of botnets attack and defense. Environment for the agent-oriented simulation was developed on the basis of OMNeT++ INET Framework.

This software simulation environment has been used for investigation of various cooperative distributed defense schemes against botnet DDoS attacks. The conducted experiments showed the availability of the proposed approach for simulation of complex botnets and defense against botnets and security analysis of projected networks. The experiments also showed that the use of cooperation of several defense teams leads to the essential raise of defense effectiveness.

The approach used in the paper allows simulating and investigating various kinds of botnets and botnet defense mechanisms. *We suppose that in the context of cyber conflicts the approach and simulation tool under development can be used for analyzing current and future defense mechanisms as well as be applied for "laboratorial" forensic investigation of botnets and network attacks fulfilled.*

Future work is related to comprehensive formal specification of botnets and defense mechanisms, deep analysis of cooperation effectiveness of various attack and defense teams and inter-team interaction, the implementation of adaptation and

self-learning defense to protect against manipulation by attackers, the expansion of attack and defense library to investigate more complicated scenarios of counteraction between botnets and botnet defense mechanisms, and the investigation of new defense mechanisms.

One of the main tasks of our current and future research is to improve the scalability and fidelity of the simulation. We now in the process of designing and experimenting with the parallel versions of our simulation environment and developing a simulation testbed combining a hierarchy of macro and micro level models of botnets and botnet defense (analytical, packet-based, emulation-based), and real small-sized networks.

The important part of future research is providing also numerous experiments to study various botnet attacks and the effectiveness of prospective defense mechanisms against botnet formation, propagation, attack detection, and response including tracing the source of attacks and botnet destruction.

ACKNOWLEDGMENTS

This research is being supported by the grant of Russian Foundation of Basic Research (# 10-01-00826-a), and the program of fundamental research of the Department for Informational Technologies and Computation Systems of the Russian Academy of Sciences (# 3.2).

REFERENCES

- Bailey, M., Cooke, E., Jahanian, F., Xu, Y., and Karir, M., 2009. A Survey of Botnet Technology and Defenses. In *Cybersecurity Applications & Technology Conference for Homeland Security.*
- Barford, P., Yegneswaran, V., 2007. An Inside Look at Botnets. In *Advances in Information Security*, Vol.27. Malware Detection. Springer.
- Binkley, J. R., Singh, S., 2006. An algorithm for anomaly-based botnet detection. In *2nd conference on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'06)*, San Jose, CA, July 2006.
- Blank, S., 2008. Web War I: Is Europe's First Information War a New Kind of War?. *Comparative Strategy*, Vol.27, Issue 3.
- Bradley, T., Harley, D., 2007. *Botnets: The Killer Web App*. Syngress Publishing, Inc. 2007.
- Chen, S., Song, Q., 2005. Perimeter-Based Defense against High Bandwidth DDoS Attacks. *IEEE Transactions on Parallel and Distributed System*, Vol.16, No.7.
- Christodorescu M., Rubin S., 2007. Can Cooperative Intrusion Detectors Challenge the Base-Rate Fallacy. *Advances in Information Security*, Vol.27. Malware Detection. Springer.
- Cohen P., Levesque, H.J., 1991. Teamwork. *Nous*, No.35.
- Colarik, A., 2006. *Cyber Terrorism: Political and Economic Implications*. Idea Group Inc.
- Dagon D., Gu G., Lee, C. P., and Lee, W., 2007. A taxonomy of botnet structures. In *Twenty-Third Annual Computer Security Applications Conference (ACSAC'07)*, Florida, USA, November 2007.
- Dunham K., Meluick, J., 2008. *Malicious Bots - An Inside Look into the Cyber-Criminal Underground of the Internet*. CRC Press.
- Gamer, T., Scharf, M., 2008. Realistic Simulation Environments for IP-based Networks. in *1st International Workshop on OMNeT++*. Marseille, France. 2008.
- Gianvecchio, S., Xie, M., Wu, Z., Wang, H., 2008. Measurement and classification of huamans and bots in internet chat. In *17th USENIX Security Symposium (Security'08)*, San Jose, CA, July 2008.
- Goebel, J., Holz, T., 2007. Rishi: Identify bot contaminated hosts by IRC nickname evaluation. In *First Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, Cambridge, MA, April 2007.
- Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., Dagon, D., 2007. Peer-to-Peer Botnets: Overview and case study. In *First Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, Cambridge, MA, April 2007.
- Grosz, B., Kraus, S., 1996. Collaborative Plans for Complex Group Actions. *Artificial Intelligence*, Vol.86, No.2.
- Gu, G., Perdisci, R., Zhang, J., Lee, W., 2008a. BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection. In *17th USENIX Security Symposium (Security'08)*, San Jose, CA, July 2008.
- Gu, G., Porras, P., Yegneswaran, V., Frog, M., Lee, W., 2007. BotHunter: Detecting malware infection through ids-driven dialog correlation. In *16th USENIX Security Symposium (Security'07)*, Boston, MA, August 2007.
- Gu, G., Zhang, J., Lee, W., 2008b. BotSniffer: Detecting botnet command and control channels in network traffic. In *15th Annual Network & Distributed System Security Symposium (NDSS'08)*, San Diego, CA, February 2008.
- Haque, N., Jennings, N.R., Moreau, L., 2005. Resource allocation in communication networks using market-based agents. *International Journal of Knowledge Based Systems*, Vol.18, No.4-5.
- Jennings, N.R., 1995. Controlling cooperative problem solving in industrial multi-agent systems using joint intentions. *Artificial Intelligence*, Vol.75, No.2.
- Kaminka, G.A., Frenkel, I., 2005. Flexible teamwork in behavior-based robots. In *AAAI-05*.
- Kaminka, G.A., Yakir, A., Erusalimchik, D., Cohen, N., 2007. Towards Collaborative Task and Team Maintenance. In *AAMAS-07*.

- Kanich, C., Lechenko, K., Enright, B., Voelker, G. M., Savage, S., 2008. The Heisenbot Uncertainty Problem: Challenges in separating bots from chaff. In *First Usenix Workshop on Large-scale Exploits and Emergent Threats (LEET'08)*, San Francisco, CA, April 2008.
- Karasaridis, A., Rexroad, B., Hoeflin, D., 2007. Wide-scale botnet detection and characterization. In *First Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, Cambridge, MA, April 2007.
- Keromytis, A.D., Misra, V., Rubenstein, D., 2003. SOS: An architecture for mitigating DDoS attacks. *Journal on Selected Areas in Communications*, No.21.
- Kotenko, I., Ulanov, A., 2006a. Agent Teams in Cyberspace: Security Guards in the Global Internet. In *International Conference on CYBERWORLDS (CW2006)*. IEEE Computer Society.
- Kotenko, I., Ulanov, A., 2006b. Agent-Based Modeling and Simulation of Network Softbots' Competition. In *Seventh Joint Conference on Knowledge-Based Software Engineering*, Amsterdam: IOS Press, Vol.140.
- Kotenko, I., Ulanov, A., 2007. Multi-agent Framework for Simulation of Adaptive Cooperative Defense against Internet Attacks. In *International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM-07)*. Springer, Vol.4476.
- Kotenko, I., Ulanov, A., 2008. "Packet Level Simulation of Cooperative Distributed Defense against Internet Attacks. In *16th Euromicro Conference on Parallel Distributed and Network-Based Processing (PDP 2008)*,
- Li, L., Alderson. D., Willinger, W., Doyle, J., 2004. A first-principles approach to understanding the internet's router-level topology. *ACM SIGCOMM Computer Communication Review*.
- Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., and Zhang, J., 2009. Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. *EURASIP Journal on Wireless Communications and Networking*, Vol.2009.
- Lopuhin, I. , Sachkov, I., 2009. *The brief analytical questionnaire on botnets in the Russian Federation for 2009 year*. March, 2009. Available at: http://www.securitylab.ru/analytics/370022.php [Accessed Feb. 15, 2010]. (in Russian)
- Macal, C.M., North, M.J., 2005. Tutorial on Agent-based Modeling and Simulation. In *2005 Winter Simulation Conference*.
- Mankins, D., Krishnan, R., Boyd, C., Zao, J., Frentz, M., 2001. Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing. In *17th Annual Computer Security Applications Conference*.
- Marietto, M., David, N., Sichman, J.S., Coelho, H., 2002. Requirements Analysis of Agent-Based Simulation Platforms: State of the Art and New Prospects. *Lecture Notes in Artificial Intelligence*, Springer, Vol.2581.
- Mirkovic, J., Dietrich, S., Dittrich, D., Reiher, P., 2004. *Internet Denial of Service: Attack and Defense Mechanisms*. Prentice Hall PTR.
- Mirkovic, J., Robinson, M., Reiher, P., Oikonomou, G., 2005. Distributed Defense Against DDOS Attacks. *University of Delaware CIS Department Technical Report CIS-TR-2005-02*.
- Papadopoulos, C., Lindell, R., Mehringer, I., Hussain, A., Govindan, R., 2003. Cossack: Coordinated suppression of simultaneous attacks. In *DISCEX III*.
- Rajab, M. A., Zarfoss, J., Monrose, F., Terzis, A., 2007. My Botnet is Bigger than Yours (Maybe, Better than Yours): why size estimates remain challenging. In *First Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, Cambridge, MA, April 2007.
- Russell, S., Norvig, P., 2009. *Artificial Intelligence: A Modern Approach* (3rd Edition). Prentice Hall.
- Strayer, W.T., Lapsely, D., Walsh, R., Livadas, C., 2008. Botnet Detection Based on Network Behavior. *Advances in Information Security*, Vol.36. Botnet Detection.
- Strayey, W. T., Walsh, R., Livadas, C., Lapsley, D., 2006. Detecting botnets with tight command and control. In *31st IEEE Conference on Local Computer Networks (LCN06)*, Tampa, Florida, November 2006.
- Tambe, M., 1997. Towards flexible teamwork. *Journal of AI Research*, No.7.
- Tambe, M., Bowring, E., Jung, H., et al., 2005. Conflicts in teamwork: Hybrids to the rescue. In *AAMAS-05*.

- Truhanov, A., 2010. Russian botnet wants to kill the competitor. 2010. Available at: http://safe.cnews.ru/news/top/index.shtml?2010/02/10/379202 [Accessed Feb. 15, 2010]. (in Russian)
- Ulanov, A., Kotenko, I., 2008. Simulation of Adaptable Agent Teams on the Internet. In *Proceedings of the 1st International Workshop on Logics for agents and mobility*
- Vishwanath, K.V., Vahdat, A., 2006. Realistic and responsive network traffic generation. In *Conference on Applications, technologies, architectures, and protocols for computer communications*.
- Wang, H., Shin, K.G., 2003. Transport-aware IP Routers: A Built-in Protection Mechanism to Counter DDoS Attacks. *IEEE Transactions on Parallel and Distributed Systems*, Vol.14, No.9.
- Wang, P., Sparks, S., Zou, C. C., 2007. An advanced hybrid peer-to-peer botnet. In *First Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, Cambridge, MA, April 2007.
- Xie, Y., Yu, F., Achan, K., Panigrahy, R., Hulten, G., Osipkov, I., 2008. Spamming Botnets: Signatures and characteristics. In *ACM SIGCOMM'08*, Seattle,WA, August 2008.
- Xuan, D., Bettati, R., Zhao, W., 2001. A Gateway-Based Defense System for Distributed DoS Attacks in High Speed Networks. In *2nd IEEE SMC Information Assurance Workshop*, West Point, NY, 2001.
- Zhou, S., Zhang, G., Zhang, G., Zhuge, Z., 2006. Towards a Precise and Complete Internet Topology Generator. In *International Conference Communications, Circuits and Systems*.
- Zhu, Z., Lu, G., Chen, Y., Fu, Z. J., Roberts, P., Han, K., 2008. Botnet research survey. In *32nd Annual IEEE International Computer Software and Applications Conference,* Turku, Finland, July 2008.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

CYBER WARFARE: AS A FORM OF LOW-INTENSITY CONFLICT AND INSURGENCY

Samuel LILES[1]

Purdue University Calumet

Abstract: Conflict and war are inherently asymmetric in their execution and planning. As Carl von Clausewitz told us, true peer competitors would rarely engage in conflict, as mutual destruction would surely occur. Throughout the later half of the twentieth century and the first decade of the twenty-first century, wars by proxy have been the primary form of super-state conflict. The technological advantage afforded by faster communications, more accurate weapons and enhanced reconnaissance is hard to ignore. It is becoming obvious that computer network attack and defense are rising in utilization within the structure of proxy war. To add to this, the super-empowered individual and small group now have access to the same militarized technologies of cyberspace as the nation-state.

Numerous models and analogies have been suggested to explain deterrence and conflict in cyberspace. Models of real-world traditional conflict though are limited in the ability to explain how the differences of terrain and weapons translate to cyberspace. As such, a low-intensity conflict – a euphemism for guerilla warfare or insurgency – is a likely wide-spectrum conflict model that may be more appropriate. Utilizing the United States military manual on counter insurgency a discussion and comparison between ad hoc militaries and militias will be developed.

This paper serves as a point of discussion on possible models of recruitment, activities and corollaries between cyber warfare and insurgency.

Keywords: strategy, conflict, cyber warfare, insurgency, counter insurgency

1 Purdue University Calumet, 2200 169th Street, Hammond, Indiana, 46304, United States email: liless@calumet.purdue.edu.

INTRODUCTION

How can a nation fight an asymmetric fight spanning a global commons while maintaining the respect and international reputation of the nation-state? That question, among others, is the fulcrum of discussion in this paper, while attempting to give a view into current work looking at strategies and tactics for nation-states to engage in cyber defense in a full-spectrum environment. Though not an empirical treatment, this paper should act as a stepping-stone into further discussion dealing with the substantial issue of non-state actors and statist proxies engaging in conflict on the cyber terrain.

To clarify, the position is not that low-intensity conflict is the only model that explains cyber warfare, or that insurgency is the only model that explains cyber warfare. Models and treatments have been attempted in the past to describe the cyber spectrum of conflict. A myriad group of theories and models have been suggested. While looking at deterrence, a nuclear weapons model of mutually assured destruction might be used to discuss the weaponization and deterrence issues (Libicki, 2009, p. 39). However, the use of the most powerful kinetic weapon does not answer what is basically a non-kinetic question. Other models of conflict might be considered such as strategic air power with the ability to harness substantial kinetic power (Rattray, 2001, p. 77). This too does not offer a substantial view into the non-kinetic nature of cyber warfare.

Some of the issue lies in what the effect of cyber warfare is. Parks (Parks & Duggan, 2001) says that cyber warfare needs to have a real-world impact of degrading, destroying, or disturbing to be relevant as a form of combat. This may be an interesting point but it may not be wholly the truth. The information operations spectrum is filled with case studies that suggest psychological actions may have relevancy as an associated capability to other more kinetic schemes. Both Clausewitz and Sun Tzu discuss in depth that the morale of the adversary may be broken, allowing winning without fighting (Hanzhang, 1987, p. 99), and troops need leadership once the battle has begun (Clausewitz, 1989, pp. 190-191).

The research question is whether a low-intensity conflict model, as found in insurgency/counterinsurgency, has an explanatory capability not currently found in other models of cyber conflict. As a problem for the networked force cyber conflict is not new. The concept of how to structure military units in the face of evolving threats is being considered deeper in other venues (Dion, 2004). This research in particular is meant to give a point of reference and open up dialog. It is not meant to stand alone and is expected to draw some criticism. As a work in progress, the expected path will be provided and some discussion will focus on the central thesis. Nation-states, corporate organizations and others that find they are fighting a

diverse and distributed adversary will find the information provided of value. Those leading multi-national forces or organizations that are already hampered by the nature of a mission to serve across national boundaries will find significant value in the following dialog.

The United States, in 1986, with the Goldwater Nichols Act ("Goldwater Nichols Department of Defense Reorganization Act of 1986," 1986) created a new definition for conflict that was other than war and instantiated the special operations command. This became known as low-intensity conflict (LIC) and among other tenets of the Goldwater-Nichols Act providing for joint operations, it provided for a set of methods to combat small wars. There already was a "Marine Corps Small Wars" manual that dated back to 1938 and dealt with counter insurgency operations. During various conflicts the concept of counter insurgency has risen to prominence and been subjugated under a variety of policy decisions. In the American experience of Vietnam and various works on the topic of insurgency, strategies can be illuminated that inform the cyber warfare and cyber conflict spectrum. A potential answer to the research question, not expected to be the only answer, is the possibility that cyber warfare being fought by a nation-state or multi-national force is a form of counter insurgency.

1. A SPECTRUM OF CONFLICT

If we accept that cyberspace is nothing more than a new type of terrain, then the entire conflict spectrum should be found within and on that terrain. It is a principle tenet of considering the terrain of cyberspace that all of the issues of society will be found on that terrain. As humans have moved from land to sea then to space, they have taken the human condition with them. As succinctly as possible, what follows is a discussion of the spectrum of cyber conflict inclusive of cyber crime (computer and communications exploitation for criminal purposes), cyber espionage (use of networks and computer systems for spying at a nation-state or at the industrial level), cyber terrorism (using communications and computer technologies to create fear) and cyber warfare (communications and computers to supplant legitimacy or replace nation-state political structures).

1.1 CYBER CRIME

Whiteside, writing in 1978, discussed in general terms a computer crime that involved the use of computers in the earlier 1970s to misdirect railroad cars worth millions of dollars (Whiteside, 1978, p. 26). This is part of a timeline that is easy to forget, highlighting that these problems are not new and have been going on

for nearly four decades. Whiteside states that in 1974 Assistant Attorney General Richard Thornburg said computer crimes came in three broad categories; 1) the computer as a victim; 2) the computer as an environment; and 3) the computer as an accomplice (Whiteside, 1978, p. 79). The technology then was only a tool. In the intervening years the model has seemingly not significantly changed.

One of the issues is that cyber crime is just crime in a new venue (cyberspace), but that it really is not new at all. Wilson argues that cyber crime is simply crime with some exceptions (Wilson, 2009, p. 417). Looking back at the discussion of different forms of crime by Thornburg, Wilson seems to be saying that the new crimes are those where the computer is the accomplice (e.g. botnets) (Wilson, 2009, p. 420). If this is true then a more holistic view of cyber crime can be taken as part of the cyberspace conflict spectrum. When looking at the incentives, it would be humorous to think that criminals would not take advantage of the computer in much the same way a shopkeeper does.

1.2 CYBER ESPIONAGE

Cyber espionage is simply espionage looking where the desired information is located. It would be silly to state that we are engaged in "file cabinet espionage" or "lockbox espionage." Lewis, discussing the incident "Titan Rain", develops a theory of cyber espionage and the issues of attribution (Lewis, 2005). As Lewis discusses, the original attribution of the espionage activities were incorrectly assessed to have originated in China. This could lead to false assumptions of attribution. Lewis cautions against jumping to conclusions too quickly. Much like darkness, the computer cloaks the spy from prying eyes, but does not mask the intruder from detection completely.

The concept of cyber espionage has a much older history found in the book by Cliff Stoll The Cuckoo's Egg (Stoll, 1990). In this case, Stoll discovered an accounting error and after many months was able to track the adversary down. This is much like regular investigations where it takes time to attribute a crime. There may be many cases of false expectations that computers will suddenly change the paradigm of investigations to a faster model.

Many authors have looked at the idea of cyber espionage, but the principle succinctly described by Lachow is that it is the use of information technology to gather information about an entity without their permission (Lachow, 2009, p. 440). In this case, Lachow is basically stating that cyber espionage is like "file cabinet espionage," but with computers and networks instead of file cabinets. Other authors have come to similar conclusions when forced to define cyber espionage. As an example, Wilson also looked at cyber espionage and follows a similar definition as Lachow (Wilson, 2009, p. 423).

1.3 CYBER TERRORISM

Verton discusses two divergent views of cyber terrorism between the professionals who are holistic in viewpoint and those who are unwilling to consider the opportunities that cyber terrorism might mean (Verton, 2003, p. 26). In many cases Verton might agree that people considering conflict are more than willing to look at a variety of the issues in an open manner. On the other hand, there are those considering conflict that have applied rule sets and are unwilling to diverge from those rule sets. This is a key insight into how insurgency is discussed later.

Quoting a definition by Mark Pollitt, Verton discusses the mistake of "pigeonholing" cyber terrorism as a primarily cyber phenomenon. The act of putting cyber terrorism in a box where it is only affecting cyber devices does not consider the larger phenomenon. A basic principle for cyber terrorism is not simply violence, but political purpose or social change in the attack. To reach a political purpose the target population must be affected in some way. As such, what Verton is discussing is that cyber terrorism is a means with results efecting human as an end.. In discussing this point, Lachow refers to cyber terrorism as the means but not the nature of the target (Lachow, 2009, p. 438). The literature is far from concrete on this issue and there are criticisms of this point. However, to consider the modes of conflict it does have an explanatory capability.

If there is cyber terrorism why do we not see it often? The argument that cyber terrorism is rare is supported by Lachow in a discussion of thousands of cyber attacks per year between 1996 and 2000 (Lachow, 2009, p. 449). With all of those attacks how many might be considered a form of terrorism? The listed attacks did not rise to the level of cyber terrorism. His assertion is that the terrorists simply were not trying or were unsuccessful in their efforts. Another point that might explain the lack of terrorism is the relationship between the adversaries. Those who might be engaged or attempting to engage in cyber terrorism simply could not create large enough effects.

2. WHY LOW-INTENSITY CONFLICT FOR CYBER WARFARE?

Low-intensity conflict is included in the conflict spectrum and used in the current networked force where cyber warfare exists. The argument over what is war and what is not war acknowledges that conflict occurs over a spectrum of action and through a variety of perception filters. The literature is rife with semantic and legal discussions on what is or is not war. The argument over different forms of "cyber" conflict has still not been answered but it has made it into the media. Whether glo-

rifying war, creating fear in the public, or simply as a plot device there is an entire genre of cinema surrounding cyber warfare and cyber terrorism.

Conway places the blame for sensationalism surrounding cyber warfare squarely on the American entertainment industry (Conway, 2007, pp. 73–74). Conversely Leonhard, discussing the principles of information warfare says a criticism exists that argues, "*··· there can be no principles governing warfare, because each situation is unique. Hence, in the purest sense of this viewpoint, we can learn no applicable lessons, nor derive any stable truth from past military events*" (Leonhard, 1998, p. 266). Though the position of Leonhard is respected, the desire is to attempt to explain principles and strategies of cyber warfare using past practices as a model. The desire in discussing cyber warfare as a form of low-intensity conflict is not to engage in sensationalism. There is also an attempt to put cyber warfare and cyber terrorism on a continuum of conflict line as reference points.

The concept of insurgency as a form of cyber conflict is not really new. Dartnell discussed the idea of web activism and global conflict in detail. Activism can rise to the level of insurgency, but rarely takes on the full aspect of war that most people would agree with. Dartnell discusses the leveling effect that interconnected networks have had and the ability to coordinate and communicate for radicalized entities (Dartnell, 2006, p. 17). This is similar to the cyber crime example earlier in this paper. Why would activists not use the same basic tools that law enforcement might use? Adaption of the tools and dual use of tools are consistent within real world insurgencies, as we will see later.

It is interesting to see that Dartnell also suggests a tribal culture, "E-nationalism", that is being noticed (Dartnell, 2006, p. 32). When we look at the population, Kilcullen has said that "real world" insurgencies have similar patterns of behavior (Kilcullen, 2009, p. 9) in how they relate within groups. It appears in real world contemporary insurgencies, that family and tribal ties lead to political motivations rather than the inverse. Dartnell positions his argument as primarily an information domain argument rather than a kinetic argument (Dartnell, 2006, p. 25). In agreement, Maura positions the argument very similarly to Dartnell and Kilcullen in the appropriated term of "hacktivism" not being to the level of terrorism (Conway, 2007, pp. 15–17; Manion & Goodrum, 2000). Hacktivism is basically the information domain equivalent of activism leading to another semantic ambiguity.

If we consider espionage as a form of conflict less than actual warfare we have specific examples of cyber engagements by military forces. Berkowitz discusses a relevant example of what a cyber espionage engagement looks like. Two super-powers engage in conflict (United States & Russia) with the United States Navy tapping (exploiting) a cable carrying military message traffic (project code named IVY BELLS) for nearly a decade (Berkowitz, 2003, p. 56). The incident is less than war but is a military action of espionage.

Berkowitz goes on to succinctly describe the balance in adversarial use of computers as weapons, *"You can do a simple attack against a lot of computers. Or you can do a sophisticated attack against a few computers. But it is really hard to do a sophisticated attack against a lot of computers, especially an attack that would achieve a meaningful military objective"* (Berkowitz, 2003, p. 147). This is part of the equation that seems to be missing in the literature. The required effort to be highly effective is balanced by the sophistication and effect. In some ways, the amended homily, "you can have effective, simple, or numbers – pick any two", seems to work as an explanation.

When considering the relative effect, it must be balanced between the technical effect and the political effect. The elements of population, adversary and terrain within a country creates a significant environment for the population of guerilla warfare to spring up (Kilcullen, 2009, p. 41). The environment can include cyberspace, but the adversary within cyberspace does not necessarily control it. The effect is what the adversary is looking for and that is consistent with terrorism and conflict in cyberspace. On balance, it is the changes in the population's perception that gives cyber conflict power.

The role and forms of warfare within society have changed substantially. There are generational warfare constructs and they appear to be of use in explaining cyber warfare. Using a generational warfare construct, Hammes discusses how, since the end of World War II, the population centric and communications strategies have changed (Hammes, 2004, p. 33). While outside the scope of this discussion, the generational constructs give a good understanding of the perception of conflict even understanding that there are criticisms (Echevarria, 2005).

Kilcullen, writing about the Pashtun tribes said, *"··· far from considering themselves part of an ordered hierarchy, members of the Pashtun tribes traditionally positioned themselves for advantage···"* (Kilcullen, 2009, p. 78). Dartnell correlates this point to the discussion on cyber activism. This correlates the concept of "real world" insurgency to the idea of cyber insurgency and thus to cyber warfare as a form of low-intensity conflict.

3. COMPARING COUNTER-INSURGENCY AND CYBER WARFARE

The United States Army and Marine Corps created a field manual to deal with counterinsurgency (FM3-24). Based on the predecessor, the *Marine Corps Small Wars Manual*, the new manual was published by Chicago University Press in 2007 (*Counterinsurgency Field Manual, 2007,* p. 2). A summary of some of the salient points

will be compared and contrasted between real world counterinsurgency and cyber conflict. Having evaluated the literature surrounding the issue, a simple comparison is achieved to help guide and produce a narrative towards cyber warfare as a form of low-intensity conflict.

Considering that conflict and the precepts of war are not completely understood or agreed upon, defining the space is important even if only for this discussion. The field manual says that insurgency and counterinsurgency (COIN) are complex subsets of warfare (*Counterinsurgency Field Manual, 2007*, p. 1). The space and or terrain of this subset is not determined or even alliterated. The same discussion could then likely be used to describe piracy as much as cyber warfare.

Once the terrain and features of the conflict are accepted then the historical aspects can be considered. It is not much surprise that insurgency has a long history as a form of conflict. There is relatively nothing new about insurgency and counterinsurgency as they have been the response of populations for a long time to conflict (*Counterinsurgency Field Manual, 2007*, p. 2). Some of the first acts in negation of policy and procedures were documented by Levy in Hackers discussing the long history of activism in the cyber realm (Levy, 1984). Conflict began within the space starting with the rise of computers and internetworked components over ideology and concerns for personal safety.

As discussed by Levy, the administrative powers took action against those who were unwilling to conform. Continuing though, we see political processes that have the nation-state pitted against nonconformists in a variety of ways. Counterinsurgency fights using all of the powers of the nation-state to apply the political, military, economic, social, information and infrastructures to the population to retain legitimacy in a complex operating environment (*Counterinsurgency Field Manual, 2007*, p. 2). This is also how the various legal systems have started to react to cyberspace.

Though the legal issues are of concern, there are direct uses other than conflict that become apparent. Much like the earlier discussion on cyber crime, real world insurgents also turn to crime to fund their activities. Insurgents have used criminal enterprise to fund themselves. This allows higher freedom of action as funding is a prime vulnerability (*Counterinsurgency Field Manual, 2007,* p. 19). This adds an additional component to the consideration of the spectrum of conflict that can be traced between the real world and cyberspace.

Cyberspace is more than just information. It is the population and their perceptions about the terrain and emotional reactions to the actions taken in cyberspace. As Kilcullen said, the population is the center of gravity (Kilcullen, 2009). The field manual mentions that information as an environment is important, but it should be realized that suicide attacks and other acts have no hope of pursuing a military victory, but

substantial value in undermining the legitimacy of government (*Counterinsurgency Field Manual, 2007*, p. 5). The response of counterinsurgents, or those trying to fight against insurgents, in cyberspace should be to maintain security and environments of trust. This raises the issue of information assurance and security as a larger policy question. Without the ability to provide security to people in cyberspace the legitimacy of government is suspect. These are consistent between cyberspace and real world counterinsurgencies.

The *Counterinsurgency Field Manual* specifically states some insurgent vulnerabilities, *"insurgents' need for secrecy, inconsistencies in the mobilization message, need to establish a base of operations, reliance on external support, need to obtain financial resources, internal divisions, need to maintain momentum, informants within the insurgency" (Counterinsurgency Field Manual, 2007*, pp. 31–32). A case can be made that these transfer in total between the "real world" and cyberspace. Financial concerns and security of operational activity are important in cyberspace too. Organizations that have used cyberspace for acts of war or insurgencies will require all of the same elements though they may be described differently. A question that could be asked is whether momentum remains the same between the two terrains. It would likely be attributed to similar if analogous needs.

4. CONCLUSIONS

Why have we not had a large-scale cyber war already? The question presupposes that it has not happened. There are reportedly thousands of attacks every day. They are not currently ascribed to political purposes. Looking at Clausewitz, we can see a large asymmetric advantage in the ability to make war already in place for the nation-state. In the case of the nation-state, would they respond to an act of aggression found in cyberspace via cyberspace or would they escalate to a kinetic response that the non-state actor (as an example) could not hope to survive? This kind of large-scale asymmetry has insulated the nation-states. Whether that can be maintained against an insurgency form of conflict may not be as clear. The principles of an insurgency are not to win a war, but to create a gap in credibility and legitimacy of the nation-state. In the information spectrum, insurgents posting videos of actions taken are not winning the war, but creating that inherent gap in credibility.

Another question is whether this model is too open or breaks rapidly under scrutiny. The insurgency and counterinsurgency models have withstood withering criticism but have risen and fallen as needs dictate. As a model in this simple overview, it has remained consistent and is shown to be part of the spectrum of conflict. It would be difficult to point to a cyber incident and find a better model than this one. As discussed earlier, specific case studies were not looked at within the scope of this

paper. Upon publication specific case studies such as the Georgia v. South Ossetia and Estonia Cyber War could be evaluated within this lens. Case studies as part of the future work would help to cement the model. At this time though, the explanatory model has little empirical evidence to support it.

The research question is answered. The model of low-intensity conflict and specifically of insurgency and counterinsurgency does have explanatory power for cyber conflict. It may not be the only model but as a model it fits with good confidence. With future work of case study analysis, the tool may be able to differentiate between simple law enforcement and cyber warfare ends of the conflict spectrum.

BIBLIOGRAPHY

- Berkowitz, B. D., 2003. The new face of war: *How war will be fought in the 21st century.* New York: Free Press.
- Clausewitz, C. V., 1989. *On War* (Indexed ed.). Princeton: Princeton University.
- Conway, M., 2007. Cyberterrorism: Hype and reality. In L. Armistead (Ed.), *Information warfare: Separating hype from reality.* Washington, D.C.: Potomac Books.
- Dartnell, M. Y., 2006. *Insurgency online: Web activism and global conflict.* Toronto: University Toronto Press.
- Dion, E., 2004. The e-Forces!: The evolution of battle-groupings in the face of 21st century challenges. *Canadian Army Journal*(7), 3.
- Echevarria, A., 2005. Fourth-generation war and other myths. Strategic Studies Institute: United States Army War College.
- Goldwater Nichols Department of Defense Reorganization Act of 1986, 99–443 C.F.R., 1986.
- Hammes, T. X., 2004. *The sling and the stone: On war in the 21st century.* St. Paul, Mn: Zenith Press.
- Hanzhang, T., 1987. *Sun Tzu's art of war.* New York: Sterling Publishing Company.
- Kilcullen, D., 2009. *The accidental guerrilla: Fighting small wars in the midst of big ones.* Oxford: Oxford University Press.
- Lachow, I., 2009. Cyber terrorism: Menace or myth? In F. D. Kramer (Ed.), *Cyberpower and national security* (pp. 437–464). Washington D.C.: National Defense University Press.
- Leonhard, R. R., 1998. *The principles of war for the information age.* New York: Presidio Press.
- Levy, S., 1984. Hackers: *Heroes of the computer revolution.* New York: Penguin Putnam.
- Lewis, J. A., 2005. *Computer espionage, Titan Rain, and China.* Washington DC: Center for Strategic & International Studies.
- Libicki, M. C., 2009. *Cyberdeterrence and cyberwar.* RAND Corporation.
- Manion, M., & Goodrum, A., 2000. Terrorism or civil disobedience: Towards a hacktivist ethic. *Computers and Society*, June, 14–19.
- Parks, R. C., & Duggan, D. P., 2001. *Principles of cyber-warfare.* Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.
- Rattray, G. J., 2001. *Strategic warfare in cyberspace.* Cambridge: The MIT Press.
- Stoll, C., 1990. *The cuckoo's egg: Tracking a spy through the maze of computer espionage.* New York: Pocket Books.
- *The U.S. Army Marine Corps counterinsurgency field manual: US Army field manual No. 3-24 Marine Corps war-fighting publication No. 3-33.5,* 2007. Chicago: University of Chicago Press.
- Verton, D., 2003. *Black Ice: The invisible threat of cyber-terrorism.* New York: McGraw-Hill/Osborne.
- Whiteside, T., 1978. *Computer capers: Tales of electronic thievery, embezzlement, and fraud.* New York: Thomas Y. Crowell Company.
- Wilson, C., 2009. Cyber Crime. In F. D. Kramer (Ed.), *Cyberpower and national security* (pp. 415–436). Washington D.C.: National Defense University Press.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

DOMAIN ENGINEERING FOR CYBER DEFENSE: A CASE STUDY AND IMPLICATIONS

Jaak TEPANDI[a], Gunnar PIHO[a,b], Innar LIIV[a]

[a]*Tallinn University of Technology, Estonia,* [b]*University of Leeds, UK*

Abstract: Efficient processing of large amounts of data gathered about real-world objects, activities, attacks, and other relevant entities is vital for successful cyber defense. The value of data processing depends critically on the quality of utilized data models. To be more practical, data models should be integrated and reused. Domain engineering addresses the challenges of model quality, integration and reuse. This paper analyses the possibilities of using domain engineering for cyber defense, exemplified and motivated by a case study of predicting the results of terrorist behavior. The presented case study demonstrates the need for adequate domain engineering for simulation and cyber defense tasks. An approach to modeling and integrating cyber defense and simulation data with archetype-based domain engineering is presented.

Keywords: cyber defense, simulation, domain engineering, modeling of terrorist behavior, archetype-based engineering

INTRODUCTION

The early motivation for this research emerged after the 1995 Oklahoma City bombing that killed 168 people. The components of the truck bomb used in this event were easily accessible to an ordinary person: ammonium nitrate, an agricultural fertilizer, and nitromethane, a motor-racing fuel. In the same way, information about usage of these and other components for preparing explosives was also easily available. The more technology develops and information spreads, the more one can expect such incidents to occur – a fact that certainly worries many people. In the study (Tepandi 2002, Tepandi&Vassiljev 2008) we modeled, simulated, and investigated a terrorism spreading problem closely related to similar issues in cyber defense.

While working on this study it soon became evident that the value of simulation results critically depends on the correctness of the world model used in simulation. Adequate methods for data representation – and more generally, for domain engineering – are also important for effective cyber defense (Presidency of the Council of the European Union (PCEU) 2009, Department of Homeland Security(DHS) 2009, Thomas&Cook 2005).

Powerful methods for domain modeling have been developed by the software engineering community (Sommerville 2006, Bjorner 2006). In the next section we outline the relationships between cyber defense and domain engineering. The second section presents a summary of the case study aimed at modeling and simulation of a terrorism spreading problem. The third section is devoted to principles of archetype-based engineering of domains, requirements, and software for cyber defense (Arlow&Neustadt 2003, Piho, et al., 2009). The final section presents some open challenges and directions for further work.

1. CYBER DEFENSE AND DOMAIN ENGINEERING

An important aspect of cyber defense is processing of large amounts of data gathered about real-world objects, activities, attacks, and other relevant entities (DHS 2009). Such data processing may give answers to specific information requests, enable mining of significant clues that help to prevent or counter cyber attacks, or provide cost-effective simulation solutions to critical information infrastructure protection (CIIP) exercises (PCEU 2009).

Efficient data processing depends critically on data representations (Thomas&Cook, et al., 2005). If the data entities are fragmented and difficult to relate to each other, then solving each new problem begins from scratch and significant data relation-

ships may be lost. In contrast, in case of integrated data representations, various objects may be associated with each other and hidden relationships may be discovered more easily. In addition, new problems may be defined and solved based on already existing world models. In (Thomas&Cook 2005, p. 133), one of the actions recommended for advancing the community's capabilities for data representation and transformation is to "create methods to synthesize information of different types and from different sources into a unified data representation so that analysts, first responders, and border personnel may focus on the meaning of the data".

Traditionally, mathematical and statistical representations are widely used to present analytical data. These representations enable efficient transformation of data to be utilized in analysis and simulation tasks. As the area to be represented widens, mathematical and statistical models tend to be less comprehensible. Therefore it is useful to utilize domain modeling experience gained in software engineering.

A proper domain model is essential for a successful realization of an information system; therefore, various representation tools and methods have been developed by the software engineering community. Requirements specified for information systems must be well agreed with the customer. Hence, significant emphasis has been put by software engineers on understandability of system models by both the developer and the customer (e.g. (Sommerville 2006, Bjorner 2006)).

As in cyber defense, different systems may reflect diverse aspects of the same domain. Therefore, it is important to have integrated domain models. In addition, the reality changes and the systems must reflect this change. Domain engineering addresses the challenges of both model integration and reuse (Bjorner 2006). It attempts to build reusable models for application domains – knowledge areas that cover important fields of reality and share common concepts. An application domain model may represent terrorism simulation, cyber defense, CIIP, medical laboratory, or other areas.

Critical IT infrastructure protection is an example of an application domain which may benefit from domain engineering. Critical IT infrastructure is important in itself, providing critical services (e.g. communications and access to vital registers). It is also vital as a supporting framework without which other critical services (e.g. banks, health services) would be impossible. Any significant future cyber conflict will most probably comprise attacks on the critical IT infrastructure. Critical information infrastructure protection (CIIP) needs to be supported by regular exercises (Enisa 2009). CIIP exercises may be expensive and sometimes impossible to perform full-scale. Simulation is a viable alternative. It cannot provide full participation experience, but enables evaluating influence, resources, consequences, and so on. Usefulness of simulation depends on the quality of data representations used and consequently – on the quality of domain modeling.

2. A CASE STUDY: AGENT-ORIENTED MODELING OF TERRORIST BEHAVIOR DYNAMICS

The application domain of the case study (Tepandi 2002, Tepandi&Vassiljev 2008) is spreading of terrorist acts. The objective of this study is to comprehend the dynamics of terrorism spreading as a function of certain world properties, such as access to information, availability of material resources, and others. The analysis is based on the indication that the probability, power, and influence of terrorist attacks – both in physical and cyber reality – are increasing with growing access to information and material resources.

2.1 MAIN HIGHLIGHTS OF THE STUDY

We begin with analyzing two extreme cases. On one extreme, when the resources, both the information and materials, are on a low level, one cannot do much harm. For example, prior the twentieth century it was practically impossible to affect the living conditions on Earth significantly by even a large number of people. In this case the probability that the population will be terminated as a result of cumulative effect of terrorist attacks may be evaluated to zero. The situation has been changed, but powerful resources have still usually been out of reach of an ordinary person. Little by little, this encouraging situation is also changing. Like in Oklahoma and subsequent events, ordinary people have more and more information and resources available for terrorism.

The other extreme is a hypothetical situation of extremely large resources being available to everyone. It seems clear that in such a case the world would not last long. There will inevitably be people who are stressed enough, or who believe that passing away is the best option for everyone. The probability that the population will cease to exist due to the cumulative effect of terrorist attacks may be evaluated to one. This extreme situation is unlikely, for the governments recognize the danger and are building barriers to available resources. Still it seems inevitable that the power in the hands of individuals is growing, and the governments are taking more measures to prevent that power from growing too high.

The study addresses the question whether the transition between the above two extremes is evolutionary (for example linear) or stepwise (for example exponential). An evolutionary transition would allow taking measures when the situation indicates that the level of resources is too high and it is time to take a more restrictive approach. In the case of a stepwise transition there might be no way back after a

certain level of resources has been exceeded.

The study involved designing the domain model for terrorist behavior, development of the simulation environment, performing simulation experiments, and drawing conclusions.

2.2 THE DOMAIN MODEL FOR TERRORIST BEHAVIOR

The domain model for terrorist behavior is based on a world of agents. The world has certain properties and so do the agents. The world evolves in a discrete time, where each unit represents a world cycle. The initial properties of the agent are determined by the world properties. The properties of each agent at the next moment are determined by the agent's individual properties, the world properties and the values of its neighbor agents at the current moment.

The world is determined by its shape and size, overall access to information and access to resources values, the level of interaction between the agents ("sociality"), initial distributions of information, resources, violence, and charity, as well as the rules for activating violence or charity acts and for changing the agent values. Example: a condition that in a specific world W, the overall value of the AccessToInformation property is in the range of 0 to 1, may be expressed by $0 \leq \text{WorldValue}(W, \text{AccessToInformation}) \leq 1$.

Some properties of the world determine characteristics of the simulation, for example the rules which determine whether the world is considered to be evolving, stable, or extinct for the purpose of analysis.

The agent properties include the amount of information and resources, as well as the levels of violence and charity. Example: a condition that for a specific agent A in the world W, the value of the AggressivenessLevel property is in the range of 0 to 1, may be expressed by $0 \leq \text{AgentValue}(W, a, \text{AggressivenessLevel}) \leq 1$.

In each world cycle, the agents go through various interactions. The agents are born and die; they acquire new and lose existing information and resources according to certain laws. The agents also perform violence or charity acts according to their property values. The nature, probability, and influence of the act depend on the agent mood, its access to resources and information, and other factors. Each violent act enlarges the aggressiveness of the neighbors and may kill other agents; each charity act enlarges the charity of the neighbors and may bring new agents into being.

An example of an agent's interaction: an object A performs a terrorist act with probability proportional to the overall violence level and its own knowledge, resources, and aggressiveness levels. As the result of the act, the neighbors of A will be removed with probability adversely proportional to the distance from A (nearer neighbors suffer to a greater extent). The Aggressiveness property of the neighbors will increase in adverse proportion with the distance from A (nearer neighbors are more influenced)

Given a world with its agents, properties, and interactions, this world may be started, letting the agents act and interact. This process may exist in a long-term or infinite continuous interaction. It may also end in termination of the population (most or all agents are destroyed as a result of terrorist attacks) or in stable non-interacting situation. The first situation occurs most probably when the opposite properties, such as violence and charity are balanced, the other two – when they are out of balance.

2.3 THE SIMULATION ENVIRONMENT

The simulation environment developed for the study provides a simulation model description language (SMDL), tools for executing the model defined in SMDL, facilities for visualizing the results of the simulation, as well as tools for saving and analyzing the results of the simulation.

The SDML defines the simulation general properties, the world general properties, the initial distribution intervals for the agent property values (Aggressiveness, Violence, Knowledge, Charity, and Resources), the rules determining change of the agent property values in each cycle, and agent properties. Example: an assertion "aggressiveness_for_act=80" specifies that if an agent's aggressiveness value is higher than 80 (on a scale 0...100) it will consider a terrorist act.

The properties defined in SDML allow a wide variety of specific populations to be simulated using the tools for executing the SDML model.

Facilities for visualizing the results of the simulation include the main window and auxiliary windows. The agents are represented as squares of different colors. The black color of a square depicts a dead agent. The other colors indicate the state of aggressiveness of an agent, varying from light green (zero aggressiveness level) to yellow (average aggressiveness) to red (very aggressive). The auxiliary windows provide graphs for average aggressiveness of the population and the number of agents alive with respect to the number of turns passed.

2.4 EXPERIMENTS AND CONCLUSIONS

At the start of a simulation run the world and the agents are specified in the SMDL. The rules for changing the world and agent properties during each world cycle are also given in SMDL. At the end of each cycle, a check is performed for the end of the simulation. The simulation run is finished and the final results are output in the following cases: the population has survived; the population has stabilized; the population has terminated.

Experiments have been performed using agent models of different complexity. In a typical experiment, the world properties, such as access to information, varied from minimum to maximum. For each intermediate value, a series of simulation runs were performed to evaluate the probability of population termination due to the cumulative influence of terrorist acts. The resulting graphs of the relationship between the world properties and the termination probability were analyzed.

The results of a typical experiment portraying the relationship between the probability of population survival and access to information for different levels of access to material resources demonstrate that the relationship tends not to be linear. Rather, the graphs represent a stepwise or constant relationship. Therefore the model does not necessarily lead to destabilization of the population with the growth of access to information. But in the case it does, the resulting dependency is rather step-wise than smooth. These experiments allow concluding that this property may be not an incidence, but regular behavior.

Thus the findings indicate that the results of terrorism activities can start spreading very quickly with the growing amount of information and material resources in individuals' hands, allowing no point of return. These results should be taken into account when designing political, social and technical systems to prevent terrorism.

The case study used both simulation and visualization for delivery of results. Simulation helps to have deeper insight into the cyber defense problems and explore risks of critical infrastructure protection situations that typically have previously not been experienced in reality. For example, as the cyber defense systems must predict behaviors and situations unspecified beforehand, simulation helps to cost-effectively predict the need for resources for these systems. Visual analytics tools and techniques help to better synthesize information, derive insight, discover the unexpected, and communicate assessment effectively for action (DHS 2009).

This case study has also demonstrated that trustworthy world models comprising terrorist activities are vital for these kinds of experiments, are complex, and require much development effort. The simulation environment must utilize multiple models for diverse tasks and experiments.

3. TOWARDS ARCHETYPE-BASED DOMAIN MODEL OF CYBER DEFENSE

The SMDL introduced in this case study is based on mathematical notations (sets, relationships, formulas) and a language for presenting the world life cycle. The practicality, integrity, and other properties of this kind of models are not easy to comprehend and analyze. To make building and analysis of domain models more feasible we propose principles of archetype-based development (ABD) (Piho, et al., 2009) for cyber defense. We use ABD at Clinical and Biomedical Proteomics Group (University of Leeds, UK) for developing software factory (Greenfield 2004) for laboratory information management system (ASTM 2006) software. In ABD we combine triptych software development (from domain via requirements to dependable software) (Bjorner 2006) with archetype and archetype patterns initiative (Arlow&Neustadt 2003).

An archetype is defined as a primordial thing that occurs consistently and universally in various domains (business, manufacturing, transportation, defense, etc.) and in systems supporting such domains. Examples of archetypes are product, feature, money, address, person, organization and so on. An archetype pattern is a collaboration of archetypes. Arlow and Neustadt have the following archetype patterns: party and party relationship, product, order, inventory, quantity and money, and rule. In the following we exemplify how to build archetype and archetype patterns based domain models for defense. These models are utilized by simulation and visualization environments to further explore critical situations and problems, as well as to obtain a deep insight that directly supports assessment, planning, and decision-making in this domain.

3.1 ZACHMAN FRAMEWORK AND ABD

Components of the ABD are represented within the Zachman Framework (ZF) (Zachman 1987, Zachman 2003a, Zachman 2003b). The ZF (Fig. 1) is a framework for enterprise architecture, which provides a formal and structured way for describing an enterprise. It is presented as a two dimensional matrix consisting of 6 rows and 6 columns. Each column of the ZF describes single, independent phenomena within the analytical target (Zachman 2003b). The rows present conceptual model, business model, system model, technology model, detailed representations, as well as functioning enterprise aspects of the domain. In what follows we characterize the contents of the columns in ZF with examples.

Column 1 (What) describes what the things are, what the features of those things are and how these things are related to each other. In ABD we use both product and

	Data Things What	Function Process How	Network Locations Where	People People Who	Time Events When	Motivation Strategy Why
	General Model of Products	General Model of Business Processes	General Model of Environment and Environment Units	General Model of Stakeholders and Their Roles	General Model of Business Events	General Model of Business Rules
Scope Conceptual model Planner Sketches	Resource, Level of Resources, Level of Knowledge, Knowledge, ...	Birth of Agent, Death of Agent, Learning, Forgetting, Earning, ...	Structure of Environment (Organization or Region for Example)	Terrorist, Informer, Agency,...	Reports About Terrorist Behaviour	"is level of aggressiveness high", "is population terminated",...
Business Model Conceptual Model Owner Drawings	Definitions of Things	Definitions of Processes	Definitions of Organization Units and their Locations	Definitions of Parties and their Roles	Definitions of Business Events	Definitions of Business Rules
System Model Logical Model Designer Architect Plans	Definitions of Things in terms of Product, Quantity and Money	Definitions of Processes in terms of Party Relationship (Feedback)	Defs of Org. Units and Locations in terms of Party and Party Relationship	Defs of Parties and Roles in terms of Party and Party Relationship	Definitions of Business Events in terms of Inventory and Order	Definitions of all Business Rules in terms of Rule
Technology Model Physical Model Builder Contractor Plans	Defs of Product, Quantity and Money Archetype Patterns	Definition of Party Relationship Archetype Pattern	Definitions of Party and Party Relationship Archetype Patterns	Definitions of Party and Party Relationship Archetype Patterns	Definitions of Inventory and Order Archetype Patterns	Definition of Rule Archetype Pattern
Detailed Representation Out-Of-Context Sub-Contractor Subcontractor Plans	Product, Quantity ... Frameworks, DLL-s, API-s and DB Tables	Party Relationship Frameworks, DLL-s, API-s and DB Tables	Party and Party Relationship Frameworks, DLL-s, API-s and DB Tables	Party and Party Relationship Frameworks, DLL-s, API-s and DB Tables	Inventory and Order Frameworks, DLL-s, API-s and DB Tables	Rule Frameworks, DLL-s, API-s and DB Tables
Functioning Enterprise Product User	Software and Services Using Product, Quantity and Money	Software and Services Using Party Relationship	Software and Services Using Party and Party Relationship	Software and Services Using Party and Party Relationship	Software and Services Using Inventory and Order	Software and Services Using Rule

Figure 1. Zachman framework with archetype patterns

quantity (Arlow&Neustadt 2003) archetype patterns for modeling things. Examples of things (derived from agent-oriented model for terrorists behavior (Tepandi 2002)) in the domain of defense can be: resource, level of resources, level of knowledge, knowledge, level of aggressiveness, aggressiveness, probability of reproduction, probability of expiration, level of access to resources, level of access to information, information, etc.

Column 2 (How) describes processes. In ABD we model processes using their feedbacks (Fig. 2) given by one party to other. We use a party relationship archetype pattern *Arlow&Neustadt 2003) for modeling such feedbacks. The examples of processes in the domain of terrorism simulation (Tepandi 2002) are birth of agent, death of agent, learning, forgetting, earning, spending, social interaction, terrorist act, charity act, etc.

These processes can be modeled as reports from one party (informer for example) to other (central agency for example) or from one party (informer) about another party (terrorist for example). More reports from trusted and different parties means better and more implicit picture about the whole process.

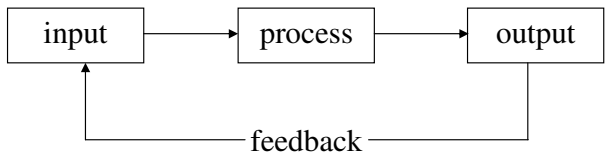

Figure 2. Process and feedback

Column 3 (Where) describes environment. School, hospital, organization, district, region, state, world, infrastructure, and computer network are examples of environments. In ABD we use party and party relationship (Arlow&Neustadt 2003) archetype patterns for modeling environments. We describe the structure of environment in terms of environment units (for instance, organizations are described in terms of organization units – division, department, team, group, etc). The role types each environment unit has to play in the environment are presented. The responsibilities (assigned, mandatory and optional), requirements for responsibilities, as well as conditions for their satisfaction for each role type and for each environment unit are depicted.

Column 4 (Who) describes the agents (persons, organizations, artificial agents) and their roles somehow related to the environment described by Column 3. In ABD we use the party and party relationship (Arlow&Neustadt 2003) archetype patterns for modeling agents and agent roles. Examples of roles of agents in domain of defense are terrorist, informer, agency, etc.

Column 5 (When) describes the events related to the processes described by Column 2. The events must be logged for audit trail or for the late analysis. In ABD we use order and inventory (Arlow&Neustadt 2003) archetype patterns for modeling events. This means that every event will generate (or will change or amend) some order to change something in the inventory. The inventory is a repository for important information about the environment. An example of an event is a report about terrorist behavior.

Column 6 (Why) describes the strategies and strategic questions such as "Is the level of aggressiveness high?", "Is the population terminated?", "Is this person a terrorist?", etc. In ABD we use the simple propositional calculus-based rule archetype pattern (Arlow&Neustadt 2003) as the basic model for strategies.

3.2 EXAMPLES OF ARCHETYPE-BASED MODELS

The following examples are archetype-based models of defense domain. For modeling of things (Column 1 in ZF) we use either product or quantity archetype patterns. As an example, for modeling agent properties like knowledge and aggressiveness, we use quantity (Fig. 3). A quantity is an amount of something characterized according to some measure and corresponding units.

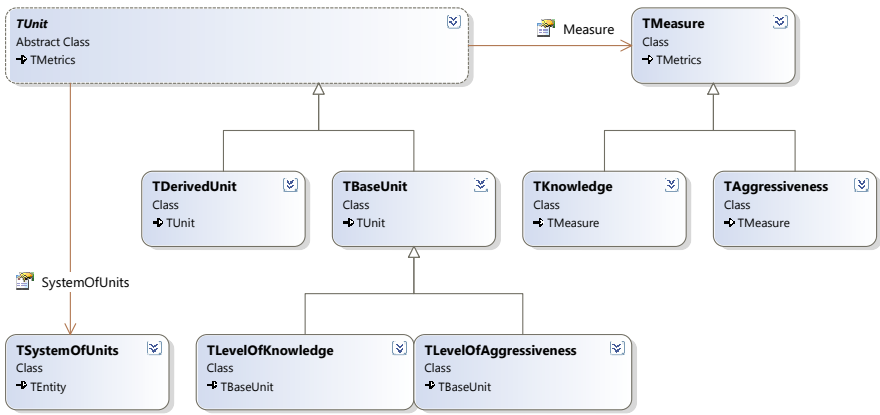

Figure 3. The agent properties

The class diagram in Fig. 3 (prefix "T" in class names comes from "type" or "archetype") comprises two measures (*TKnowledge* and *TAggressivness*) and two units (*TLevelOfKnowledge* and *TLevelOfAggressivness*). Both units are inherited from the *TBaseUnit*. As a result, the units inherit automatically the functions associated with the base unit such as arithmetic operations (addition, subtraction, and so on), round-

ing, or translation of quantity from one unit to other.

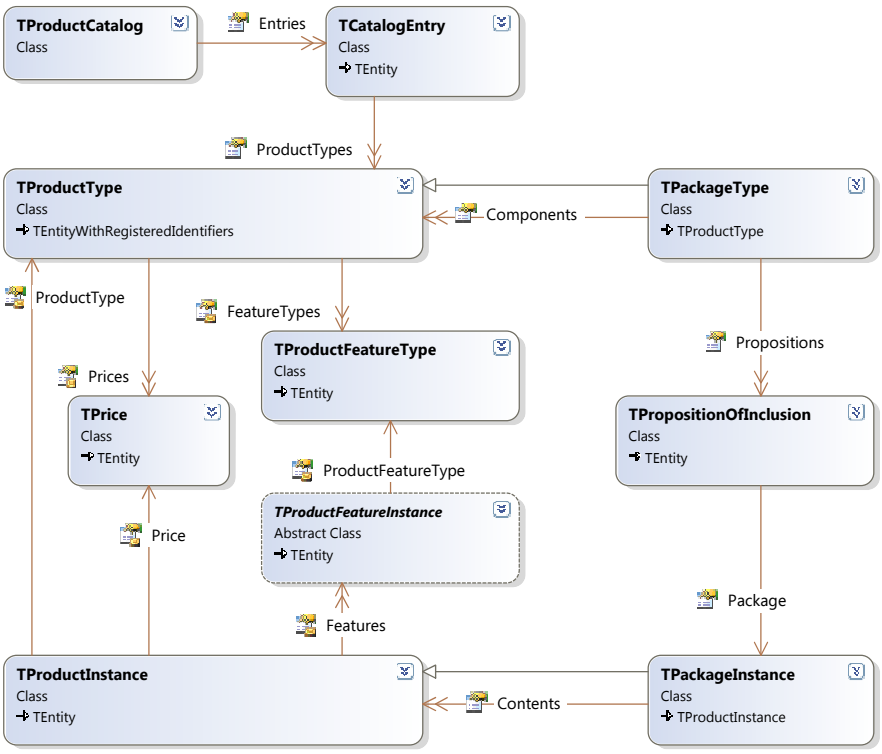

Figure 4. Product archetype pattern abstraction

Some objects in the domain of defense, for example agent resources, are different kinds of products and/or services. All those things that an agent can in principle buy or sell can be modeled by using the product archetype pattern (parts of this pattern are presented in Fig. 4). *Product type* describes the common properties of a set of goods or services and *product instance* represents a specific instance of a product type. *Product feature type* and *product feature* are used either to represent possible product type features (like set of possible colors) or to represent concrete features of specified product instance. Packages (*package type* and *instance* respectively) are selections of products grouped together as a product unit. *Components* in *package type* are used when a package consists of a fixed set of products; a *product set* is used to represent a set of *product types* from which selection by some rule may be made. A *product relationship* is a relationship (upgrade, substitute, replace, complement, compatible, and incompatible) between product types. A *price* is the amount of money that must be paid in order to purchase a product. A product type has pos-

sible *prices* whereas the product instance has an *agreed price*. The *pricing strategy* determines how a price is calculated for a package type. Product *catalog* is a store of product information where *catalog entry* holds the information about a particular type of product in a product catalog. Similarly, a *batch* describes a set of product instances of a specific product type that must be tracked together, for example, for quality control purposes.

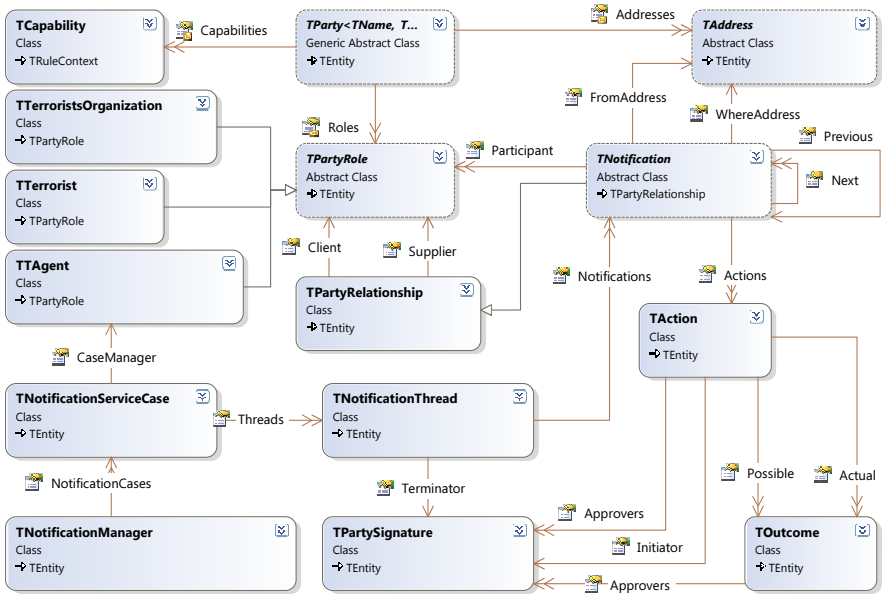

Figure 5. Notification archetype pattern abstraction

For modeling of processes (Column 2 in ZF) we use the party relationship archetype pattern as a base. For example the notification archetype pattern (Fig. 5) concretizes the party relationship archetype (Arlow&Neustadt 2003) and is similar to the customer relationship management archetype pattern (Arlow&Neustadt 2003). In notification, the agent (*TAgent*) "from" address notifies about some event which has happened in the "where" address. In case of terrorism simulation, this may be a party relationship where one agent informs the agency about the behavior of the terrorist's organization or about the behavior of someone who acts on behalf of a terrorist's organization. More than one terrorist or terrorist's organization – participants – can be involved in event the about which the agent has reported. A notification routing is a special case of notification, which represents notification handovers from agent to agent. Notification case tracks all notification threads (sequence of notification) about a specific topic related to a specific terrorist's organization or terrorist. Action represents something that can or must happen (logging of information

or some other action for example) after the notification.

Notifications and actions (logging of information) these notifications generate may be, for example, information about birth (new member of a terrorist's organization or new terrorist's organization), death (death of a terrorist or terrorist's organization), earning (terrorist or terrorist's organization has got more resources), learning (terrorists have got new information) and so on.

For modeling of the environment (Column 3 in ZF) we use the party and party relationship (Arlow&Neustadt 2003) archetype patterns. The *party archetype* (Fig. 6) represents a (identifiable, addressable) unit that may have a legal status and has some autonomous control over its actions. *Persons* and *organizations* are parties.

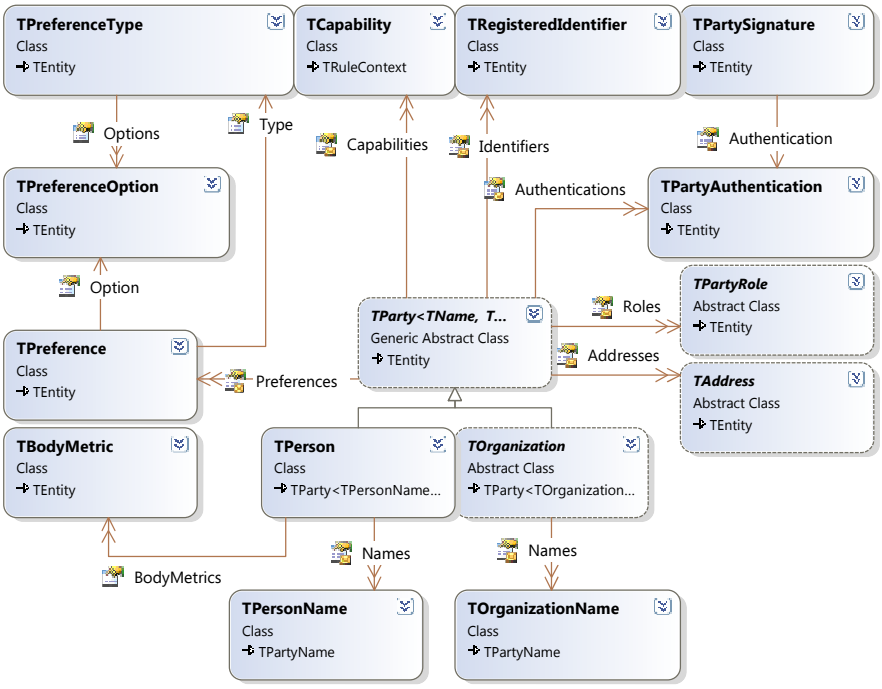

Figure 6. Party archetype pattern abstraction

Party has zero or more *addresses* (phone number, e-mail, web address, postal address) where one and the same address can belong to more than one parties. Party has zero or more *registered identifiers* (passport, VAT number, domain name, stock exchange symbol, etc). Party *authentication* is a way to confirm that the party is who they say they are. Each party can play different *roles* (one and the same person can be for example a student and a member of terrorist's organization). *Preference*

stands for a party's (or a role's) choice of or linking for something (like dietary preference) and is typically selected from a set of options. The *capability* is a collection of facts about what a person or organization is capable of doing as well as *body metric* stores information about the human body. For example the world global properties (Tepandi 2002) like *InitialPopulation, GlobalEndOfPopulation, GlobalAccessLevelToInformation,* etc., are capabilities of a party called the world (set of agents).

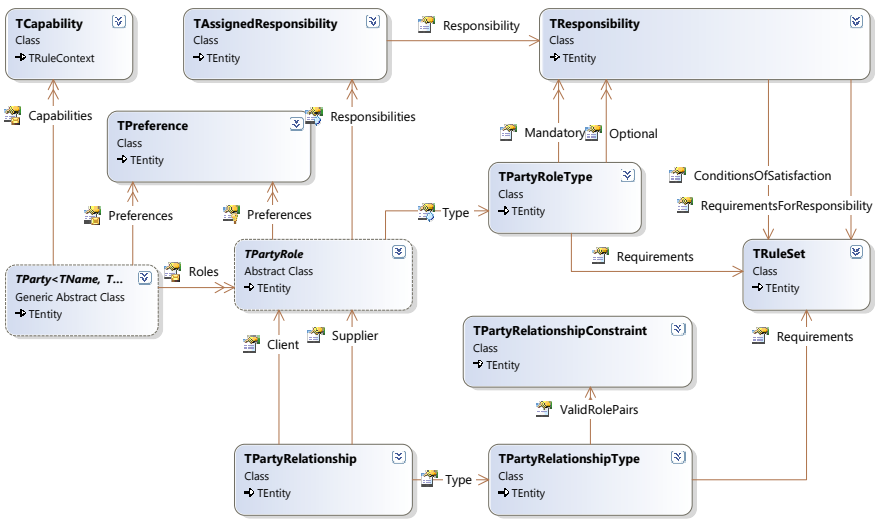

Figure 7. Party relationship archetype pattern abstraction

Fig. 7 abstracts the *party relationship archetype pattern*, which captures a fact about the semantic relationship between two parties in which each party plays a specific role. Binary (more flexible and cleaner than n-ary) relationship is used, which means that one *relationship* binds two roles called "client" and "supplier". It has to be clarified that the role is always solely used to store information that belongs to the role itself and not either to a party or to a relationship. *Role type* is used to store common information for a set of similar roles; *relationship type* is used to store common information for a set of a similar relationship instances. *Responsibility* describes a particular activity that a party, playing a role, may be expected to perform, where the *assigned responsibility* captures the fact that responsibility is assigned to concrete party playing that role. *Conditions of satisfaction,* as well as the *requirements* for *party role type*, for *party relationship type* and for *responsibility* are *rule sets* (see rule archetype below). Here the *capability* (rule context) contains information needed for the execution of rules; in case of a party, this information states whether a party can complete necessary responsibilities for its role in relationship. In ABD we use party relationship archetype pattern for modeling of internal structure (for

example all immobile under the defense) and chains of command in the environment.

The same party and party relationship archetypes are used for modeling of persons (Column 4 in ZF). While in the case of Column 3 (location) the target is to model the environment where the business takes place, in case of Column 4 we model all the stakeholders somehow active or related to the business in question.

Although the location and stakeholder-related domain aspects are both modeled by the party relationship archetype pattern, these models themselves are different. In the case of locations we use the party relationship archetype pattern to model the internal structure of the environment, for example the organizational structure of the enterprise. In the case of stakeholders, we model specific employers, customers, sellers, patients, terrorists and other independent agents with their relationships with the environment in question. We also model the possible relationships between independent agents (e.g. employer A is wife of employer B, and so on).

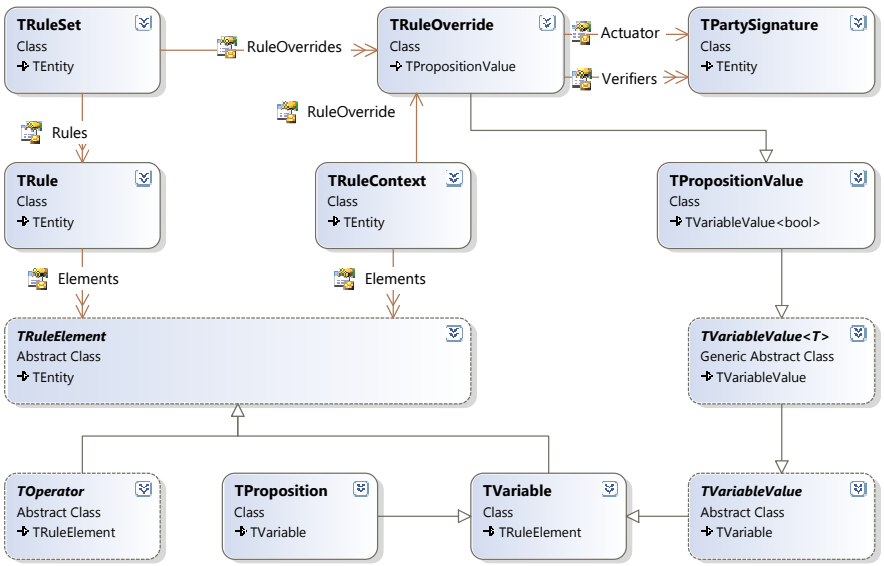

Figure 8. Rule archetype pattern abstraction

The processes (Column 2 in ZF) comprise actions. These actions are triggers for events modeled by Column 5 of ZF (when). For modeling of events, we use the order and inventory archetype patterns. An action generates a document. This document is some type of order, and according to this order, the inventory of environment (Column 3) will be updated.

The last column of ZF (why) describes strategies. For modeling strategies, we use rule archetype patterns. A *rule archetype pattern* (Fig. 8) is a constraint on the operation of the software systems of the business. The rule semantics is defined by sequence of *rule elements*. Rule elements can be *operators*, *propositions* (a statement that has a truth value) and *variables*. Operator is either a Boolean operator (and, or, xor, not) or quantifier operator (=, !=, <, >, <=, >=). While a *rule* represents some kind of mask or pattern, the *rule context* contains the informational context for the execution of a rule. Rule context represents this information as a collection of rule elements that may be propositions or variables, but not operators. The following sets are examples of simple rule (R) and respective rule context (C) (Arlow&Neustadt 2003).

R = {IsGoldCardHolder, IsSilverCardHolder, OR,
CarryOnBaggageKg, AllowedBaggageKg, LESS, AND}
C = {true, false, 4.5, 5.0}

IsGoldCardHolder and *IsSiverCardHolder* are propositions which take the actual value from the context C (true and false, respectively). *CarryOnBaggageKg* and *AllowedBaggageKg* are variables which take the actual values (4.5 and 5.0) from context. OR, LESS and AND are operators.

3.3 FROM DOMAIN VIA REQUIREMENTS TO SOFTWARE

The triptych software process (Bjorner 2006) – from domain model via requirements to software – has a very simple informal description: before starting to write software, we need to know the requirements; before knowing requirements, we have to understand the domain; to understand the domain we have to study one. The interpretation on ZF rows in terms of triptych (requirements, domain, and software) development can be as follows.

Row 1 (conceptual model) is just the glossary (list of things, objects, assets, etc.) that defines the scope or boundary of requirements. For example the cell defining the scope for Column 4 (people) for the domain of defense can include terms like *agent*, *terrorist*, *informer*, *agency*, and so on.

Row 2 (business / semantic model) is a definition and a model of the actual requirements. It defines the concepts (terms and facts) actually needed. This can be represented as simple narratives (for instance "terrorist has an alias", "informer has a codename", etc.) or in some more formalized (for example class diagrams) notation.

Row 3 (system / logical model) describes the requirements in terms of domain

model. For Column 4 this means for example, that "terrorist is the role for person", "terrorists alias is a name for person whose role is a terrorist", etc.

Row 4 (technology / physical model) is the actual model of the domain. For Column 4 this is the model of the party archetype pattern.

Row 5 (detailed definition) is the party archetype pattern realized for example as API, or as a database scheme supporting this pattern under some specific database engine.

Row 6 (product) is the software or service which fulfils the requirements from row 1 and row 2.

Due to the technological infrastructure and nature of attacks, it is possible to have two strategies for implementation of cyber defense domain engineering. One approach is to model the normal behavior in systems with a goal of detecting abnormal events, behavioral outliers, etc. Another, complementary approach is to model specific attack types (e.g. DDoS attacks (Mirkovic&Reiher 2004, Douligeris&Mitrokotsa 2004)). Archetype-based domain engineering allows simultaneously both top-down (building models from existing taxonomies of attacks) and bottom-up (generalizing data-driven models from detailed event logs) approaches. Archetypes representing normal behavior of the system and a specific attack must be described in a way to allow semi-automatic synthesis of simulation procedures.

4. CONCLUSIONS

We have described a case study of predicting the results of terrorist behavior, stressed the need for adequate domain engineering for simulation and cyber defense tasks, and proposed an approach to integrating cyber defense and simulation data representations using domain engineering with archetype-based domain engineering.

As open challenges and directions for further work, the cyber defense domain can be viewed as an integration of object and process views. Domain engineering for the processes and integration of object and process representations are some directions for further work.

This work was partially financed from ESF grant No. 6839 and target financing grant SF0140013s10.

REFERENCES

- Arlow, J., Neustadt, I., 2003. *Enterprise Patterns and MDA: Building Better Software With Archetype Patterns and UML* : Addisson-Wesly.
- ASTM. 2006. *E1578-06 Standard Guide for Laboratory Information Management Systems (LIMS)* : ASTM International.
- Björner, D., 2006. *Software Engineering, Vol. 3: Domains, Requirements, and Software Design.* Texts in Theoretical Computer Science, the EATCS Series : Springer.
- C. Douligeris, C. and A. Mitrokotsa, A, 2004. *DDoS Attacks and Defense Mechanisms: Classification and State-of-the-art*, Comp. Networks, vol. 44, pp. 643–66.
- Department of Homeland Security. 2009. *National Infrastructure protection Plan.*
- ENISA. 2009. *Good Practice Guide on National Exercises. Enhancing the Resilience of Public Communications Networks.*
- Greenfield, J., et al., 2004. *Software Factories: Assembling Applications with Patterns, Models, Frameworks, and Tools* : Wiley.
- Mirkovic, J. and Reiher, P., 2004. *A taxonomy of DDoS attacks and defence mechanisms. ACM SIGCOMM Computer Communications Review, 34(2):39–54, Apr. 2004.*
- Piho, G., Roost, M., Perkins, C., and Tepandi, J., 2009. Towards Archetypes Based Software Development. *CISSE.* (accepted for publication).
- Presidency of the Council of the European Union., 2009. "Conference conclusions." Tallinn : s.n., 27-28 April, 2009. European Union Ministerial Conference on Critical Information Infrastructure Protection.
- Sommerville, I., 2006. *Software Engineering.* : Addison-Wesley.
- Tepandi, J. and Vassiljev, S., 2008. Conflict Expansion in an Information Rich Society: Feasibility of Corrective Actions. [ed.] E. Khaled. *Innovations and Advanced Techniques in Systems, Computing Sciences and Software Engineering* : Springer, pp. 231-236. ISBN 978-1-4020-8734-9.
- Tepandi, J., 2002. Simulation of Conflict in an Agent World: Access to Resources and Possibility of Termination of the Population. *Informatica.*, Vol. 13, 4, pp. 501-512.
- Thomas, J. J. and Cook, K. A., 2005. *Illuminating the Path. The Research and Development Agenda for Visual Analytics.* : National Visualization and Analytics Center.
- Zachman, J. A., 1987. A Framework for Information Systems Architecture. *IBM Systems Journal.* Vol. 26, 3.
- Zachman, J. A., 2003b. *The Zachman Framework: A Primer for Enterprise Engineering and Manufacturing.* 2003b.
- Zachman, J. A., 2003a. *The Framework for Enterprise Architecture – Cell Definition.* ZIFA .

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

ESCAPING THE CYBER STATE OF NATURE: CYBER DETERRENCE AND INTERNATIONAL INSTITUTIONS

Ryan T. KAMINSKI[1]

Columbia University, New York, USA

Abstract: The existing literature related to cyber security tends to conclude that states cannot rely on so-called 'cyber deterrence' to prevent cyber attacks. A little analysis, however, discusses why this is the case and if cyber deterrence can ever be a practical national or international security strategy. Analyzing four cases of cyber attacks against states, this paper isolates three variables acting to hinder cyber deterrence including the lack of a cyber legal lexicon, difficulty in tracing cyber attacks, and too low levels of transparency when establishing national cyberwarfare policies. It is argued such factors can be manipulated via the use of international institutions as evidenced by the existence of the Chemical Weapons Convention, Nuclear Non-Proliferation Treaty, and certain aspects of the post-9/11 Bush Doctrine. The task before states then, is to re-think purely domestic approaches to cyber security.

Keywords: cyber warfare, international institutions, cyber deterrence, international organizations, national security

Disclaimer: This research was performed under an appointment to the U.S. Department of Homeland Security Scholarship and Fellowship Program, administered by the Oak Ridge Institute for Science and Education through an interagency agreement between the U.S. Department of Energy and DHS. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE, or ORAU/ORISE.

1 Columbia University School of International and Public Affairs, 420 West 118th Street, New York, New York, 10025, Email: rtk2107@columbia.edu.

INTRODUCTION

In an editorial. David Tohn (2009), National Security Fellow at Harvard's Kennedy School of Government, compares cyberspace with Thomas Hobbes' chaotic state of nature arguing, "The world of cyber-crime, cyber-terrorism, and cyber-warfare is truly a wild, unruly, and ungoverned place" (p. 17). Another study from the Center for Strategic and International Studies (CSIS) argues that cyber security currently presents one of the "most urgent national security problems" facing the US (Lewis, Langevin, McCaul, Charney, & Raduege, 2008). A RAND Corporation commission concerning cyber security concludes, *"deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace"* (Libicki 2009). Overall, the majority of literature on the emerging concept of cyberwarfare seems to follow a more or less similar pattern of reasoning.

Specifically, articles and reports on the subject tend to sound the alarm, deploy a titillating term like 'cyber-vigilantes,' and pessimistically conclude that states cannot expect to rely on a Cold War-inspired state of deterrence. Other literature commonly focuses on cyber crime and cyber terrorism against the private sector, giving comparatively little attention to the possibility of cyber attacks among states. Given that the respected computer security company McAfee estimates that as of 2007 at least 120 countries were engaging in research to use the internet for war fighting purposes, the US and NATO, if not the entire world, faces a growing threat (Takeda, Ferraro, Edwards, Blum, & Vaile, 2007, p. 12). Unfortunately, a scant amount of literature discusses in detail what specific factors act to preclude grafting the notion of deterrence onto the concept of cyberwarfare. Consequently, only minimal discussion has emerged concerning whether such variables can be manipulated.

To fill this conceptual gap, I examine four cases of cyber attacks and how they highlight the difficulties of relying on deterrence to prevent or mitigate the use of cyber attacks between states.[2] The cases include cyber attacks against Estonia in April 2007, cyber attacks against Georgia in August 2008, the worldwide 'GhostNet' attacks occurring between May 2007 and March 2009, and the string of cyber attacks against South Korea–US interests in July 2009.[3] Analyzing these cases, I find three main factors currently preventing states from relying on cyber deterrence. They include: the lack of a comprehensive legal lexicon regarding cyber attacks; no return address for those individuals, groups, and states committing cyber attacks; and too little transparency and public debate when crafting national cyberwarfare policies.

---

2 The term "cyber attack" is used in order to remain as neutral as possible concerning what is and what is not an act of cyberwar, cyber espionage, etc.

3 Most computer servers remain unaware they have been infected by GhostNet. The March 2009 date refers to the last *recorded* infiltration.

It is argued that while such factors present significant obstacles for creating an international strategic environment where cyber deterrence is possible, they are not insurmountable. Specifically, past international accords and norms such as the Chemical Weapons Convention (CWC), Nuclear Non-Proliferation Treaty (NPT), and particular aspects of the post-9/11 Bush Doctrine provide convincing evidence that an international institutional approach, rather than the conventional 'one-state one-policy' framework, presents the most efficacious path for establishing a foundation for cyber deterrence.

1. FOUR CASES

1.1 ESTONIA – APRIL 2007

Beginning on April 27, 2007, a series of coordinated distributed denial of service (DDoS) attacks were launched primarily against Estonia's government-run websites. Many analysts have speculated that the Estonian government's decision to move a Cold War-era statue motivated the cyber attack ("Estonia Fines," 2008). With Estonia's Parliament declaring online access a human right in 2000 as well as Estonia being considered "one of the world's most wired countries," the attack carried the potential to severely disrupt everyday cyber activity in the country (Brookes, 2008).

Despite Estonia's considerable emphasis on its citizens having internet access, however, the April 2007 DDoS attacks did not cause significant damage to Estonia's infrastructure or government websites. Rather, the attack caused temporary access-related problems for Estonians attempting to view webpages such as the website of the Prime Minister's political party (Sanger, Markoff, & Shanker, 2009, p. 1). A fake apology for relocating the Cold War memorial was also allegedly posted on the Prime Minister's webpage (Wickramarathna, 2009). Elsewhere, other government-sponsored links were corrupted to misdirect users to iconic pictures of Soviet soldiers and quotations from Martin Luther King, Jr. about fighting evil (Wickramarathna, 2009).

Later, Estonian Foreign Minister Urmas Paet would publicly accuse Russia of sponsoring the attack, but would later admit that neither Estonia nor NATO had any direct evidence to support such a claim (Wickramarathna, 2009). In January 2008, an ethnic Russian-Estonian college student was tried and convicted for carrying out part of the attack on the Estonian Reform Party's website and fined around $1,350 ("Estonia Fines," 2008).

1.2 GEORGIA – AUGUST 2008

Early in its August 2008 war with Russia regarding the breakaway territories of South Ossetia and Abkhazia, Georgia was a victim to a host of cyber attacks also allegedly emanating from Russia. Specifically, two rounds of DDoS attacks were launched against Georgian government websites as well as respected Georgian media outlets. Several private websites such as *StopGeorgia* were also established complete with easy-to-use software for caring out DDoS attacks ("Marching," 2008).

According to the *Economist*, however, the "actual damage done was minimal: some e-mail was disrupted and targeted websites were rendered unavailable to the public" ("Marching," 2008). The genuine significance of these acts, however, is hard to measure as other countries including the US, Estonia, and Poland mirrored Georgia's original government websites (Korns & Kastenburg, 2009). Absent such assistance, the official US Army website found that Georgia risked becoming "cyber-locked" or having no access to the internet (Korns & Kastenburg, 2009).

Once again, Russia would claim it was not involved in the attacks ("Georgia Targeted", 2008). Most analysts seem to agree that Russian nationalists were responsible for the attack using BOT or "zombie" networks to facilitate the DDoS campaign ("Georgia Targeted," 2008). Whether such individuals received assistance directly from Moscow remains unclear.

1.3 GHOSTNET – MAY 2007 THROUGH MARCH 2009

Contrasting from the attacks on Georgia and Estonia were the massive so-called 'GhostNet' attacks which occurred globally over a 22-month period between 2007 and 2009. According to researchers at Toronto University's Munk Centre for International Studies 1,295 computers in 103 countries were allegedly infiltrated ("Chinese Ghost," 2009). Unlike the cyber attacks targeting Estonia, however, most analysts conclude that one of the most important features of the GhostNet attacks concerned its power to whisk away potentially sensitive information using a combination of phishing and malware strategies.

One study conducted at the University of Cambridge Computer Laboratory firmly points the finger at Chinese authorities for operating GhostNet, as the Tibetan government in exile was a key target of the cyber attacks ("Chinese Ghost," 2009). A joint Toronto University and Ottawa think-tank research group also reportedly found evidence that the Tibetan government's computer system had been corrupted to send relevant Tibet-related information back to servers in China, but did not di-

rectly accuse the Chinese government of carrying out the attack (Jacobson, 2009).

In response, an official from the Chinese government declared, "I will not be surprised if this report is just another case of their recent media and propaganda campaign" (Harvey, 2009). Another problem with putting the blame for the GhostNet attacks on China is the fact that the software used to infiltrate various foreign websites and government officials' email accounts was discovered to be available online using a Google Search (Kelly, 2009). It is also unclear what strategic motivation China would have to steal information from states and entities targeted in the attack such as Barbados, Malta, Cyprus, Portugal and Hong Kong.

1.4 SOUTH KOREAN & US INTEREST ATTACKS – JULY 2009

The last case concerns a concentration of attacks in July 2009 overwhelmingly targeting South Korean and US government and military interests. Beginning on July 4th, the attacks occurred in three waves primarily relying on a DDoS strategy. Specifically, the websites of the US White House, National Security Agency, Federal Aviation Administration, State Department, Secret Service, Treasury, Federal Trade Commission, and South Korea's National Intelligence Service were targeted (Siobhan & Ramstad, 2009). Compared to other small-scale cyber attacks, the *Wall Street Journal* notes that the July 2009 cyber attacks "were among the broadest and longest-lasting assaults perpetrated on government and commercial Web sites in both countries" (Siobhan & Ramstad, 2009).

Once again, general expert opinion seems to conclude that damage associated with the attacks was minimal. Jose Nazaro (2009), manager of security research at Arbor Networks, notes, "The code is really pretty elementary . . . I'm doubting that the author is a computer science graduate student" (Sang-Hu & Markoff, 2009). A White House spokesperson also claimed the attacks had "absolutely no effect on the White House's day-to-day operations" (Sang-Hu & Markoff, 2009). It is worth noting, however, that the US Treasury Department's, Trade Commission's, and Department of Transportation's websites were all briefly shut down during the attack ("US Eyes").

While a recent South Korean investigation cites North Korea as the perpetrator, an opposition South Korean political party claims such findings are little more than a callous attempt by one agency to increase its power and influence within the South Korea government (Sang-Hu & Markoff, 2009). Although some officials have noted the attacks almost perfectly overlapped with North Korean missile tests and a UN Security Council resolution passed against the country, there is little conclusive evidence linking North Korea to the attacks (Siobhan & Ramstad, 2009). One North

Korean embassy official claimed that rumors of North Korea's involvement in the cyber attacks were baseless (Siobhan & Ramstad, 2009).

2. VARIABLES AFFECTING CYBER DETERRENCE

The four cases consistently point to three key variables that preclude states from relying on cyber deterrence. They include the absence of a cyber legal lexicon, difficulty in determining the source of cyber attacks, and low levels of transparency and genuine public discussion on the subject of cyberwarfare strategy and defense. In this section each variable will be clarified.

2.1 LACK OF A UNIVERSALLY ACCEPTED CYBERWARFARE LEXICON

Anyone reading lay articles, think-tank studies, published manuscripts, or even government reports on cyber attacks is likely to find a dizzying array of terms sometimes referring to the same concept. For example, should a DDoS attack that causes disruptions to a government website, yet does not steal any sensitive information, be considered an act of cyberwar, cyber espionage, or cyber vandalism?

The implications of lacking a generally accepted vocabulary in this area are twofold. First, depending on what lexical framework is used, international and customary law can be interpreted to permit vastly different reactions to the same cyber attack. For example, if two states have contrasting lexicons concerning cyberwarfare, one could view a cyber attack as an act of war, while the other could conceptualize it merely as an act of cyber vandalism ("Marching Off," 2008). Second, given that some states even lack a universally accepted cyber glossary among their various domestic civilian and military agencies, the possibility of misinterpreting a potential cyber attack on the national level also remains high (Shanker & Markoff, 2009).

Looking at the Estonian and Georgian cases, this problem is uniquely apparent. Tohn (2009), for one, hyperbolizes the attacks against both states as "cyber-blitzkriegs," regardless of such a term's connotation with an all-out military attack from World War II (p. 17). Former US Deputy Assistant Secretary of Defense Peter Brookes (2008) even classifies the attack on Estonia as a "pre-emptive digital strike" despite the lack of any significant evidence that Estonia was planning a cyber attack on Russia. Jaak Aaviksoo, Estonia's Defense Minister, also declared that the cyber attack against his country "cannot be treated as hooliganism, but has to be treated as an attack against the state" ("Marching Off," 2008). Even though Estonia did not end up

invoking Article V of the NATO charter which commits states to treat an attack on one member as an attack on themselves, the defense minister's comments nonetheless illuminate major problems associated with the lack of a comprehensive cyber-warfare lexicon. While Estonia did construct a NATO-sponsored facility in its capital to study cyber security, this also may do little good if non-NATO members like China and Russia are relying upon an entirely different cyber language.

Similarly, while many respected media outlets referred to the cyber attacks against Georgia as acts of 'cyberwar', other analysts have concluded that this is not the case, as the attacks did not cause any "physical harm" ("Marching Off," 2008). Others, however, counter that the attacks on Georgia can still be considered 'cyberwarfare' as they were accompanied by a military offensive ("Marching Off," 2008).

In a similar vein, classification of the GhostNet attacks as activity related to a "global spy network" or as an act of 'cyber espionage' remains in dispute (Jacobson, 2009). For example, a critical legal difference may exist between a cyber attack that merely downloads information or one that actually takes control of sensitive computers. Arguing GhostNet was capable of the latter, the Information Warfare Monitor (IWM) group clarifies, "The GhostNet system directs infected computers to download a Trojan known as Ghost Rat that allows attackers to gain complete, real-time control" (Harvey, 2009, p. 29).

While the cyber attacks committed against South Korea and the US raise issues similar to the Estonian and Georgian cases, the former case also posits questions concerning what a proportional response to a cyber attack should be. Given that several government websites went down in the US, it is difficult to hypothesize what an appropriate US response would have been had it known with certainty that North Korea committed the attacks. A recent high-level US panel on the subject of cyber attacks, for example, noted its concern over a disturbing 2004 Pentagon statement on a similar scenario. Notably, the Pentagon statement claimed that in the event of a cyber attack, "on US commercial information systems or attacks against transportation networks" the US should consider the use of nuclear weapons (Shanker & Markoff, 2009). Additionally, while the 2010 US nuclear strategy rules out nuclear retaliation in response to cyber attacks, it delineates exceptions for certain states including Iran and North Korea (Sanger & Baker, 2010, p. A1).

2.2 DIFFICULTY IN DETERMINING THE ORIGINS AND/OR PERPETRATORS OF CYBER ATTACKS

Another inherent problem with cyber deterrence concerns difficulty in determining who is committing the cyber attack. If the attacker is not a state, another question to

answer concerns to what extent states have a responsibility to prevent or investigate attacks committed by non-state actors operating within their sovereign territory. According to US Deputy Defense Secretary William J. Lynn III, "Deterrence is predicated on the assumption that you know the identity of your adversary, but that is rarely the case in cyberspace, where it is so easy for an attacker to hide" (Waterman, 2009, p. B01).

While many signs seem to point to Moscow in the Estonia and Georgia cases, there is still no hard public evidence that Russia committed the attacks ("Marching Off," 2008). James Lewis (2009), Director of the CSIS Technology and Public Policy Program, disputes the notion that countries—including Russia—cannot stop cyber attacks from being executed within their territory:

> *We should not forget that many of the countries that are havens for cyber crime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control. The notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government is difficult to accept.*

Similar charges have been made against China regarding GhostNet. In, *Tracking GhostNet,* Robert Deibert notes, "The most significant actors in cyberspace are not states. In China, the authorities most likely perceive individual attackers [i.e. teenagers in internet cafés] as convenient instruments of national power" (Jacobson, 2009). Another headache for determining who was responsible for the GhostNet attacks concerns the fact that the software associated with GhostNet was easily accessible to virtually any internet user. One cyber security analyst told a reporter, "It's a nice piece of software – easy interface . . . You can do it yourself" (Kelley, 2009).

Finally, the July 2009 attacks on South Korea and US interests raise complex issues regarding infected 'zombie' computers around the globe inadvertently participating in cyber attacks against other countries. Specifically, South Korea's spy agency concluded computers from 16 different countries participated in the DDoS attacks. Rafal Rohozinski, an investigator for IWM, further notes, "Attribution is difficult because there is no agreed upon international legal framework for being able to pursue investigations down to their logical conclusion, which is highly local" (Sanger et al, 2009).

2.3 INADEQUATE TRANSPARENCY AND PUBLIC DISCUSSION ON CYBERWARFARE

Further precluding the possibility of cyber deterrence is the high amount of secrecy concerning cyberwarfare-related policymaking. Overall, this has especially been true for the US. Many international security analysts, for example, have noted a growing hypocrisy on the part of the US in criticizing the stealthy cyberwarfare policies of other states like China and Russia while remaining incredibly secretive about US cyber policy (Glenny, 2008). Marcus Sachs, who helped to establish one of the first government cyberwarfare units in the US, argues, "We need to have a public debate, not a classified conversation" (Waterman, 2009).

The US Cyber Consequences Unit also conducted a comprehensive study of the cyber attacks targeting Georgia. Problematically, though, only certain portions of it were made public (Fulghum, 2009).[4] The group's conclusions—as described by an anonymous IT official familiar with the group's work—included the idea that the cyber attacks against Georgia had "direct" benefits for Russia's military (Fulghum, 2009). Given such a revelation, it is unfortunate the report was not made public and able to contribute to the already limited public literature on the implications of integrating cyber attacks with traditional military operations.

Next, while no firm evidence has solidly linked China to the GhostNet cyber attacks, many have nonetheless faulted China's lack of military transparency especially in the area of cyber security. Bill Gertz (2008), a journalist with the *Washington Times*, claims anonymous Pentagon sources have discovered that "There is growing evidence ... that rather than simply adopting Western-style military secrecy, China's military is engaged in a wider effort at denial and deception." The same Pentagon officials further clarified that one of the most non-transparent areas of the Chinese military concerns cyberwarfare (Gertz, 2008).

On the other side of the Pacific, the US has been critiqued for lacking a public and coherent cyber doctrine in the wake of the July 4th cyber attacks. According to a *Washington Post* editorial published eights days after the attacks began, "lack of a guiding vision has implications beyond mere inefficiency. The nation's cyber-defenses are being developed without any structure to guarantee transparency and accountability" ("Cyber czar," 2009, p. A10). Another report conducted by a high-level panel organized by the National Academy of Sciences entitled "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities,"' also finds that a lack of open discussion about cyberwarfare within the US could have significant negative effects for US military policy (Shanker & Markoff, 2009). Moreover, while the South Korean National Intelligence Service claimed it was

4 A summary of the US Cyber Consequences Unit report on the 2008 cyber attacks against Georgia was made public and can be found in the bibliography under Borg and Bumgarner.

extremely likely that "North Korea" or "North Korean sympathizers" were behind the attacks, and no evidence was provided as it had been deemed "classified" ("U.S. Eyes," 2009).

3. THE CASE FOR AN INTERNATIONAL APPROACH

This section shows that the three cyber deterrence variables have successfully been manipulated in the past through the CWC, NPT and Bush Doctrine. It will also present evidence that the current approach to cyber security is problematically overwhelmingly centered at the national level, particularly in the US.

3.1 A NATIONAL SECURITY ISSUE

By and large, the world's preeminent military power, along with other major powers, has focused on the development of a cyberwarfare strategy on the national level rather than the international. This, however, must change if the possibility of cyber deterrence being a reasonable option for states—rather than a scenario where states just attempt to dominate the cyberwarfare landscape or engage in cyber arms races—is to exist. One US military officer argues, "The fortress model simply will not work for cyber . . . Someone will always get in" (Sanger et al, 2009, p. 1). While bilateral or regional agreements toward this end should generally be considered a step in the right direction, they carry similar problems associated with the current one-state, one-policy approach to cyber attacks.

At the UN, the US and its allies have balked at Russian attempts to construct a cyber attack treaty from a belief that such an accord would merely protect states lacking the capacity to engage in cyberwarfare (Adams, 2001, p. 104). Larry McKee, an adviser to US Strategic Command, however, believes such reluctance may be more logistics-related. He notes, "There are so many stakeholder organizations and individuals in the cyberdomain it is difficult to know exactly where to start the collaboration, information sharing, and integration" (Waterman, 2009). On the other hand, the existence of a UN Convention on Cyber crime and a comparable EU accord show the notion of a cyberwarfare treaty is not entirely without precedent. Additionally, Geoffrey Darnton (2006), Head of Knowledge Transfer for the Institute of Business and Law, finds that the 1977 Geneva Protocol may provide a foundation for the regulation of cyberwarfare as it specifically expands the jurisdiction of the accord to include "new weapons . . . means or method[s] of warfare" (p. 147).

Others, however, have posited that it may be best to start regionally. Duncan Hollis,

a law professor at Temple University, finds regional organizations like NATO or the EU should first formally clarify a set of cyber attack standards amongst themselves ("Marching Off," 2008). Again, while such a development would not be negative per se, problems could still arise if different regional organizations or states have clashing cyber lexicons. Several Russian military officers have reportedly endorsed the doctrine that "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself" (Hildreth, 2002, p. 13-15). James Lewis (2009) clarifies the implications of the national versus international cyber security problem:

> *We have, at best, a few years . . . to modernize our laws to allow for adequate security . . . The United States will need to define doctrine for the use of the cyber attack as a tool of national power. It would benefit from an effort to reshape the international environment for cyber conflict in ways that could reduce risk, to win consensus (as we did with proliferation) on a set of norms and constraints for cyber conflict ("Korean Cyber attacks").*

3.2 CHEMICAL WEAPONS CONVENTION

Opened for signatures in January 1993, the CWC presents startling evidence of the success of the international community's ability to regulate specific types of warfare. Regarding the accord's global effect, James Caroll (2008) with the *Boston Globe* eloquently summarizes, "The 1993 convention has been ratified by almost every nation on Earth . . . Their [chemical weapons] legitimacy has been entirely removed, their permanence rejected. The poison gas realists of 1919 have been proven wrong" (p. A15). According to David Cooper (2002) in *Competing Western Strategies against the Proliferation of Weapons of Mass Destruction*, "the mere existence of a legal prohibition provides a meaningful disincentive for covert possession by participants, despite a low probability of detection" (p. 27).

Beyond mere symbolism, the CWC contains a tri-level lexicon for understanding what can and cannot be considered a chemical weapon subject to the convention's regulations. This includes Schedule 1, 2, and 3-type weapons, along with criteria for determining what chemicals fall under what Schedule and specific disarmament- related obligations ("Article 1 Obligations"). Article II of the CWC also lays out accepted interpretations for chemical weapons-related components as well as for verification instruments ("Definitions and Criteria").

Next, the CWC contains provisions not only regarding what acts are prohibited by the treaty, but also obligations for states not to transfer chemical weapons to non-state actors. In particular, the convention demands that state-parties actively work

to prevent the use of chemical weapons. Article I, for example, orders members of the convention not "to develop, produce, otherwise acquire, stockpile or retain chemical weapons, or transfer, directly or indirectly, chemical weapons to anyone" as well as not "to assist, encourage or induce, in any way, anyone to engage in any activity prohibited to a State Party under this Convention" ("Article 1 Obligations").

3.3 NUCLEAR NON-PROLIFERATION TREATY

Opened for signatures in July 1968, the NPT has been signed by 189 countries and constitutes the foundation of the international nuclear non-proliferation regime. US President Obama's recent demand for renewed efforts towards universal nuclear weapons disarmament at a special session of the UN Security Council presents a testament to the strength and durability of this accord (Kessler & Sheridan, 2009). Overall, the NPT provides substantial evidence that establishing a cyber legal lexicon as well as increasing transparency concerning cyberwarfare is possible.

For example, the NPT distinguishes "nuclear weapon states" from "non-nuclear weapon states" while also clarifying what sorts of nuclear technology the latter are and are not entitled to receive (IAEA, 1970). Another little discussed norm associated with the treaty concerns nuclear weapon states agreeing not to employ their weapons against non-nuclear states unless the latter allies with a nuclear state or uses a nuclear weapon which it recently acquired (Kimball, 2005). While some nuclear states have recently stretched this perceived rule in regard to the targeting of nuclear weapons and declaratory policies, Kimball (2005) notes that this has only been done for 'rogue' states (2005).

Another growing norm associated with the NPT concerns obligations to prevent terrorists from acquiring nuclear weapons. The effect has been the establishment of new multilateral agreements like the 2003 Proliferation Security Initiative (PSI) designed to prevent the proliferation of nuclear materials and other weapons of mass destruction. Mark Shulman, (2006) with the Strategic Studies Institute, notes that the PSI "has received widespread support . . . United Nations Secretary-General Kofi Annan has explicitly endorsed it . . . at least 60 nations are participating in it."

Pertaining to transparency, the NPT calls upon non-nuclear weapon states to submit to IAEA inspections. While critics will likely point out that certain countries have ignored such provisions, the IAEA nonetheless has been able to carry out investigations in Iraq, Iran, and North Korea in the past. While the occasional nuclear weapons breakout scenario has occurred, the normative power associated with the IAEA and NPT has still inarguably invalidated former President Kennedy's prediction that there would be 15-20 new nuclear weapon states by 1970 (Allison, 2004).

3.4 THE BUSH DOCTRINE

While international scholars continue to debate the efficacy of the Bush Doctrine, in terms of US foreign policy, one aspect of it as declared in September 2001 before a joint session of the US Congress, is uniquely applicable to the second variable acting to preclude cyber deterrence. President Bush stated,

> *"We will pursue nations that provide aid or safe haven to terrorism. Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists. From this day forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime" (Whitehouse, 2001).*

This statement places an affirmative obligation on states to prevent non-state actors from operating and launching attacks from within their territory. While many US foreign policy experts and historians have critiqued this part of the Bush Doctrine as representing a radical departure from previous international law, it seems for better or worse to have been accepted by many key players at the international level. Russia, for example, has invoked the doctrine in its ongoing struggle with Chechnya, and Israel has used it to justify its numerous incursions into Palestinian territories (Diehl, 2002, p. A21). Some political pundits in the US have even argued that the Obama Administration's recently enunciated policy towards Pakistan resembles a tacit endorsement of the Bush Doctrine ("Matalin," 2009).

4. CONCLUSION

While Tohn offers a pessimistic view of contemporary cyber security reminiscent of Hobbes' hellish state of nature, he forgets that Hobbes ultimately concludes that individuals lacking any sense of industry or justice will eventually come together and empower a Leviathan to rescue them from such chaos. There is no doubt that neither the UN nor any other currently existing intergovernmental organization remotely resembles a Hobbesian Leviathan, but this is not to say that a cooperative international approach is entirely impractical when linked to cyber attacks.

On the contrary, factors inhibiting the implementation of cyber deterrence strategies including the lack of a cyberwarfare lexicon, difficulty in tracing cyber attacks to their state or non-state origins, and a lack of transparency can and must be addressed at the international level rather than merely the national. Past international agreements and norms such as the CWC, NPT, and certain aspects of the Bush Doctrine provide convincing evidence that cyber deterrence can be a possibility given that states are willing to commit the political muscle to do so. If an international

cyber security regime with widely accepted norms and procedures concerning cyberwarfare can be built, the costs of 'cheating' will radically increase, making the execution of shadowy cyber attacks a less and less tantalizing option for states. The probability of a cyberwar instigated by miscalculations or accidents will also drop as nations will have a forum to discuss their disputes. Finally, states will also have an incentive to preemptively detect, target, and neutralize non-state groups wishing to carryout cyber attacks from within their territory rather than just looking the other way. The challenge now is for states to recalibrate their cyber security policies from the national to international arena.

REFERENCES

- A Chinese Ghost in the Machine: Cyberwarfare. 2009, April 4. *Economist.*
- A. Guidelines for Schedules of Chemicals . (n.d.). *Organisation for the Prohibition of Chemical Weapons.* Retrieved February 4, 2010, from http://www.opcw.org/chemical-weapons-convention/annex-on-chemicals/a-guidelines-for-schedules-of-chemicals/
- Adams, J., 2001. Virtual Defense. *Foreign Affairs, 80*(3).
- AFP. (2008, August 12). AFP: Georgia targeted in cyber attack. *Google*. Retrieved February 4, 2010, from http://afp.google.com/article/ALeqM5iRuGsssizXAKVgmPqAXOxqB5uHsQ
- About the Convention. (n.d.). *Organisation for the Prohibition of Chemical Weapons*. Retrieved February 4, 2010, from http://www.opcw.org/chemical-weapons-convention/about-the-convention/
- Allison, G. 2004, January 1. Nuclear Terrorism - FAQs. *Nuclear Terrorism: The Ultimate Preventable Catastrophe - Home*. Retrieved February 4, 2010, from http://www.nuclearterror.org/faq.
- BBC, 2008, January 25. *Front Page*. Retrieved February 4, 2010, from http://news.bbc.co.uk/2/hi/technology/7208511.stm
- Borg, S. & Bumgarner J., 2008. Overview of the US-CCU of the Cyber Campaign Against Georgia in August of 2008. US Cyber Consequence Unit. Retreived April 5, 2010, from http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf
- Brookes, P., 2008, March 4. The Cyber Challenge. *The Heritage Foundation - Conservative Policy Research and Analysis*. Retrieved February 4, 2010, from http://www.heritage.org/press/commentary/ed031008c.cfm
- Carroll, J., 2008, June 23. If Poison Gas Can Go, Why Not Nukes. *Boston Globe.*
- CNN, 2009, December 6. Matalin: With AfghanistanSurge: Obama Resembles George W. Bush. *CNN.* Retrieved February 4, 2010, from politicalticker.blogs.cnn.com/2009/12/06/matalin-with-afghan-surge-obama-resembles-george-w-bush/.
- Cooper, D. A., 2001. *Competing Western Strategies Against the Proliferation of Weapons of Mass Destruction: Comparing the United States to a Close Ally.* Westport, CT: Praeger Publishers.
- Diehl, J., 2002, April 29. Free Pass on Chechnya. *Washington Post.*
- Fulghum, D., 2009, September 14. Cyberwar is Official . *Aviation Week & Space Technology, 171,* 0.
- Geoffrey, D., 2006. Information Warfare and the Laws of War. In D. Webb Ed. *Cyberwar, Netwar and the Revolution in Military Affairs* (pp. 139-151). New York: Palgrave Macmillan.
- Gertz, B., 2008, August 21. Plugged In--National Security. *Washington Times.*
- Glenny, M., 2008, June 26. Cyber armies are gearing up in the cold war of the web. The Guardian.
- Harvey, M., 2009, March 30. Chinese hackers 'using ghost network to control embassy computers.' *Times Online.* Retrieved February 4, 2010, from http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece
- Hildreth, S., 2001. Terrorism and the Future of US Foreign Policy. In J. Blane Ed. *Cyberwarfare: Terror at a Click (*pp. 1-22). New York: Novinka Books.
- Jacobson, S., 2009, March 31. China denies involvement in GhostNet cyber-attacks *The First Post.* Retrieved February 4, 2010, from http://www.thefirstpost.co.uk/46883,news-comment,news-politics,china-denies-involvement-in-GhostNet-cyber-attacks
- Kelley, C., 2009, March 31. Cyberspies' code a click away. *Toronto Star*. Retrieved February 4, 2010, from http://www.thestar.com/article/610860
- Kessler, G., & Sheridan, M. B., 2009, September 24. Security Council Adopts Nuclear Weapons Resolution. *Washington Post*. Retrieved February 4, 2009.
- Kimball, D., 2005, February 15. The Future of the Nuclear Non-Proliferation Regime. *Arms Control Association* . Retrieved February 4, 2009, from https://www.armscontrol.org/events/20050219_AAAS

- Korns, S., & Kastenbeg, J., 2009. Georgia's Cyber Lefthook. *Parameters, 38(4)*. Retrieved February 4, 2010, from http://74.125.93.132/search?q=cache:http://www.usamhi.army.mil/USAWC/Parameters/08winter/contents.htm
- Levy, C., 2009, May 27. In Siberia, the Death Knell of a Complex Holding a Deadly Stockpile. *New York Times.*
- Lewis, J., Langevin, J., McCaul, M., Charney, S., & Raduege, H., 2008. Securing Cyberspace for the 44th Presidency. *Center for Strategic and International Studies.* Retrieved February 4, 2009, from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
- Lewis, J., 2009, October 1. The "Korean" Cyber Attacks and Their Implications for Cyber Conflict | Center for Strategic and International Studies. *Center for Strategic and International Studies.* Retrieved February 4, 2010, from http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict
- Libicki, M., 2009, December 1. Cyber deterrence and Cyberwar. *RAND Corporation.* Retrieved February 4, 2009, from http://www.rand.org/pubs/monographs/2009/RAND_MG877.sum.pdf
- Marching off to cyberwar., 2008, December 6. *Economist (US).*
- Membership of the Biological Weapons Convention. (n.d.). *The United Nations Office at Geneva.* Retrieved February 4, 2010, from www.unog.ch/80256EE600585943/(httpPages)/7BE6CBBEA0477B52C12571860035FD5C?OpenDocument
- MSNBC., 2009, July 2. U.S. eyes N. Korea for 'massive' cyber attacks. *MSNBC.* Retrieved February 5, 2010, from http://www.msnbc.msn.com/id/31789294
- President Declares "Freedom at War with Fear", 2001, September 20. *Welcome to the White House.* Retrieved February 4, 2010, from http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html
- Sanger D., Baker, P., 2010, April 6. Obama Limits When US would Use Nuclear Arms. *New York Times.*
- Sanger, D., Markoff, J., & Shanker, T., 2009, August 28. US Plans Attack and Defense in Web. *New York Times.*
- Sang-Hu, C., & Markoff, J., 2009, July 9. Cyber attacks jam government and commerical websites in U.S. and South Korea. *New York Times.*
- Siobhan, G., & Ramstad, E., 2009, July 9. Cyber Blitz Hits US, South Korea. *Wall Street Journal.*
- Shulman, M., 2006, April 1. The Proliferation Security Initiative as a New Paradigm for Peace and Security. *Strategic Studies Institute.*
- Takeda, K., Ferraro, M., Edwards, G., Blum, R., & Vaile, D., 2010, February 5. 2007 Virtual Criminal Report: The Next Wave. *McAfee Corporation.* Retrieved February 1, 2010, from http://www.mcafee.com/us/local_content/reports/mcafee_criminology_report2007_en.pdf
- Tohn, D., 2009, June 11. Digital Trench Warfare. *Boston Globe.*
- Treaty on the Non-Proliferation of Nuclear Weapons. (1970, April 22). *International Atomic Energy Agency.* Retrieved February 4, 2010, from http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc140.pdf
- Waterman, S., 2009, July 2. U.S. takes aim at cyberwarfare. *Washington Times.* Retrieved February 5, 2010, from http://www.washingtontimes.com/news/2009/jul/02/us-takes-aim-at-cyberwarfare/
- Wentworth, T., 2008, August 23. How Russia May Have Attacked Georgia's Internet. *Newsweek.* Retrieved February 4, 2010, from http://www.newsweek.com/id/154965
- Where is our Cyber czar?, 2009, August 12. *Washington Post.*
- Wickramarathna, W., 2009, August 27. Online edition of Daily News. Retrieved February 4, 2010, from http://www.dailynews.lk/2009/07/27/fea02.asp

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

FROM PITCHFORKS TO LAPTOPS: VOLUNTEERS IN CYBER CONFLICTS

Rain OTTIS

CCD COE, Tallinn, Estonia

Abstract: The capability and mandate for organized violence in the international setting has normally been the domain of nation-states. Cyberspace, however, provides an international arena where almost anyone has the power to attack any target at will. While most of these attacks have little effect, there is often little disincentive to using them, as attribution of cyber attacks and effective punishment of attackers is still the exception, instead of the norm. Thus, 21st century farmers with pitchforks or cyber militia become more than a local force and, if organized well enough, can mount an offensive cyber campaign that affects a nation-state on the other side of the planet.

In order to test this claim, I will consider the potential threat from the Internet users who are untrained in hacking techniques and who have very limited resources. In general, there are two types of activities that are open to such persons: supporting the cyber campaign by providing resources, cover and training (among other things) and launching cyber attacks as part of the cyber campaign. It is important to note that an untrained individual is probably more useful when providing support to skilled attackers, instead of actually participating in the cyber attacks.

Based on the overview of the simple options that are available for a novice cyber attacker, I will draw some conclusions on the actual threat posed by a (ad-hoc) cyber militia of amateurs.

Keywords: patriotic hacking, hacktivism, cyber militia, cyber attack, cyber conflict

INTRODUCTION

The emergence of the Internet has transformed the way ordinary citizens can take part in global politics. On the one hand, information from political conflicts can be relayed in near real time to people who are interested in the conflict. On the other hand, people can take part in shaping the conflict from their homes, regardless of the distances involved, because cyberspace has become a new medium for political activism. This may manifest as an information dissemination campaign in support of or against some political entity. However, it can also take the form of a politically motivated cyber attack campaign by patriotic hackers or hacktivists.

Recent international conflicts have often been accompanied by virtual side-conflicts that mirror the underlying political situation. While such events took place as early as the 1990s, they have become more common and widespread over the last decade (Denning, 2010). Usually these virtual campaigns cannot be directly attributed to any state, although it is often clear which state(s) the attackers support. Instead, there seems to be a trend of (anonymous) private citizens forming into on-line militia groups to perform cyber attacks against political opponents (Carr, 2009; Nazario, 2009).

It is important to note that even if there are no official ties between a government and an on-line cyber militia, the government may still use the militia as an instrument of state power. This approach would provide deniability and allow the state to distance itself from the attacks (Ottis, 2009).

Carr (2009) has identified that many active participants of cyber campaigns display very little training and experience. In other words, around a core group of experienced hackers there are a large number of untrained attackers. This is similar to some medieval campaigns, where a group of well-trained and equipped knights were supported by untrained and poorly equipped peasants. Arguably, this has led to the phrase "farmers with pitchforks", which describes an amateur force. Let us extend this phrase to the twenty-first century, by providing the notional farmers with another easily accessible and necessary tool – the laptop.

In order to increase the understanding of the threat posed by a group of these low-level militiamen, I will first define them by minimum required skills and resources. I will list several options that are available to such individuals both for participating in the cyber attack campaign, as well as supporting it, assuming that they have access to a communications channel where more experienced persons can provide them with tools and advice. Finally, I will draw some conclusions about the threat posed by these so-called "farmers with laptops".

1. "FARMERS WITH LAPTOPS"

Obviously, the low-end membership of an on-line cyber militia does not need to consist of farmers. The real issue is that they are neither trained for "cyber combat", nor is hacking a serious hobby for them. They are merely drawn to a political conflict and are motivated and willing to contribute their effort and resources to make a difference via cyberspace. Let us first define the skills and resources that such attackers can be realistically assumed to have.

1.1 HACKER ZERO – SKILLS

The people in question are assumed to have no special training or experience with cyber attacks, but they should be familiar with basic computer use. Therefore, it should be fairly safe to assume that they at least know how to use:

- *A web browser.* Specifically, they need to be able to navigate to websites (if they have the link or know the address), run simple queries on search engines, post content in forums, as well as download files from a website (link) to their computer.
- *An e-mail client or a web interface for e-mail.* Simple operations like writing and sending an e-mail with attached files to a given e-mail address.
- *Basic features of the operating system on the computer that they will use (most likely a version of Microsoft Windows).* Basic features include opening/executing and copying files, as well as installing software with default settings ("Next – Next – Next") and copying/pasting information between different applications (from web browser to command prompt).

1.2 HACKER ZERO – RESOURCES

It should be safe to assume that the attackers have access to at least:

- *A personal computer.* For example a laptop with the operating system mentioned above and a web browser.
- *Internet access.* This access does not need to be fast, nor constantly available. For example, access to public WiFi could be enough.

Since the militia is expected to consist of volunteers, not direct representatives of a government or commercial entity, we cannot assume "corporate sponsorship", although it is likely that some members have control over commercial or government-owned systems. For the purposes of this work, however, a basic computer with an Internet connection is sufficient.

2. BASIC OFFENSIVE ACTIONS

Since *cyber attack* was not listed in the skill set, they must first find some information. A simple web search query will provide plenty of potential attack methods. More than likely, a search result will also point to specialized forums that discuss cyber attack techniques. If the person is a member in a group that considers a cyber campaign, then it is enough if only one of them finds the information – he can then share it with the rest. A more likely scenario is that someone in the group has a deeper understanding of conducting cyber attacks (including choice of correct targets and tools) and can provide the necessary information (or links to it) himself.

At this stage, the militia members have used the skills and resources at their disposal to gain access (either searching the web or communicating online via e-mail or web forum, etc.) to simple cyber attack instructions and tools. Let us analyze some potential options available for them, bearing in mind that this is not the complete list of possible options, but merely a sample of approaches.

2.1 MANUAL (DISTRIBUTED) DENIAL OF SERVICE

A Denial of Service (DoS) attack abuses some vulnerability in the target or supporting infrastructure to make it unavailable for normal use. Usually this is achieved by exhausting the resources of the target or by disabling the target by exploiting a logic flaw in the system. Assuming that the instructions and tools are shared in the interested community, we get many people from different locations performing the DoS. In effect, the cyber militia becomes a human botnet that is launching a distributed denial of service (DDoS) attack. Let us consider some very basic ways to attempt a denial of service attack.

A simple way to generate extra network traffic for a website is to continuously refresh the website in the browser (for example, by holding down the F5 key while at the website). Another way to accomplish this is to continuously click through links in the website (opening them in tabs) without actually taking the time to look at it. These are not designed as attack features, but they can be used to attack the server nevertheless. They tie down the resources of the target (processing power, bandwidth, memory) by over-using legitimate services. In order to be effective, however, many attackers must coordinate their actions for the duration of the attack.

Yet another way is to send email (with attachments, or with very long text, or with malware). A single person will most likely not be able to have a serious effect on an e-mail server. However, thousands of people doing it at the same time may actually have a significant effect. Especially considering that they are sending e-mail from

many different addresses (source blocking will not work in the beginning) and with very different content (automated content scans will be of limited use).

One can also misuse the ping command, which is a basic tool for network administrators. There have been examples of attack instructions that basically tell the user to open the command prompt and paste a pre-written ping command (with longer packet length and specified number of attempts) in it (Ottis, 2008). Once the user hits enter, his computer starts sending out a steady stream of packets (ICMP ECHO) to the target system in order to exhaust its resources. Again, this approach requires a large number of people.

These are just a few of the simpler methods to attack the target system. While any one of them is too weak to achieve much alone, they could become a serious availability problem, if coordinated and performed by a large group.

2.2 DoS SCRIPTS AND ATTACK KITS

While manual DoS attacks can be easy to do, they require time and effort, especially if one wants to maintain pressure on the target. However, this problem is easily mitigated by automation. In the same websites and forums, where manual attack instructions are available, people can usually find automated attack tools (Carr, 2009; Ottis, 2008).

Simple script files can be downloaded and executed on the attacker's computer. For example, the script can automate the pinging process explained above. The attacker only needs to start the script once and the computer will continue to attack the target on its own.

Furthermore, specialized attack tools can be disseminated via website or forum. For example, there are programs that can be used for generating various types of network traffic (including http traffic). All one needs to do is to download it, start the program, insert the target address and start the attack. Often there are also easy ways to customize the attack (traffic type, packet size and frequency, etc.) by ticking the necessary boxes and inserting the necessary values.

This type of attack is much more powerful than the manual attack, as it can result in much more "attack traffic" per attacker and it can last longer. It is also important to note that the attackers do not have to write any code, nor do they have to understand how the data packets are created, routed and processed. All they need to do is to download a program and use it.

2.3 WEB DEFACEMENT

Web defacement refers to an attack where the perpetrator gains unauthorized access to the web server and changes the content of the website. While this requires knowledge and experience beyond our defined set of attackers, there are still ways for an untrained person to perform a web defacement attack.

Some web server vulnerabilities allow the attacker to make the web server execute (exploit code) files that are located on a third party server (so-called cross site scripting). For example, this could be done by adding a customized text string (provided by someone else) to the target web address in the web browser's address bar. Note that this type of attack is highly reliant on specific vulnerabilities in the code or configuration of the target server. It only works if the system is unpatched or if there is no patch available or if the system is configured so it allows the exploit to run. Therefore, it is highly unlikely that this type of attack works on a specific target server. However, the attacker may try this approach on a large number of servers and may have success on some of the servers.

Once again, it is possible to automate this process. A program may cycle through a set of differently "customized" web addresses on a range of target websites. The web site can be defaced, if even one automatically detected vulnerability is present at the target. In the end, the attacker only needs to download and start a program, add the payload (for example, a text that will be displayed on the defaced site) and potential target addresses and start the attack. Note, again, that this attack is best suited for sweeping a broad set of targets, but is probably not effective against a small target set.

There are many other ways to deface a website. However, the chance of success for an untrained attacker is quite low, so web defacement most likely remains a tool for specialized attackers. For example, the web portal Zone-H.org maintains a list of reported web defacement attacks that are likely performed by specialized attackers.

2.4 MALWARE ATTACK

Introducing malware to the target system is another method that is available for an untrained attacker. While they are not able to write the malware themselves, they can download it from the web and then deliver it to the target.

The simplest way would be to just e-mail the malware to the users of the target system. However, this may not be effective, as the malware can be identified and neutralized (deleted, quarantined, etc.) by anti-virus software before it reaches the victim. Furthermore, the malware may not work in the system, because it targets a

vulnerability that is not present. For example, the target could be running a different operating system or a different mail client (or whatever application's vulnerability is targeted).

Another simple way would be to send the victim an e-mail enticing him to download the malware (masquerading as something else) or to visit a web site that automatically attempts to infect the victim's system (a so called drive-by download).

Yet another way is to deliver it to the target system manually. If the attacker has access to the system, he may copy or download the malware directly to the system (insider attack). However, a safer way to do it would be to "lose" a data carrier (USB memory stick, CD, etc.) where the victim may find it or to mail it to the victim as something else (with a plausible explanation, using social engineering techniques, to dispel any doubt on behalf of the victim). This way, the victim will circumvent the boundary protection mechanisms of the system and introduce the vulnerability at his workstation.

The malware itself could be configured to achieve many objectives, ranging from covert information collection to systematically corrupting all data in the system. During a crisis situation, this approach could have serious consequences for the organization that owns the system.

2.5 INTELLIGENCE GATHERING

All the examples in this section provide potential intelligence value. DoS and DDoS can be used to test the bandwidth or some other capacity of the target system. Defacement and malware attacks allow the attacker to collect information about the system itself, the data in it and its users.

3. SUPPORT ACTIONS

In addition to carrying out cyber attacks, there are many ways to support a cyber attack campaign. While these support actions may not create any direct damage or consequences, they can have a strong influence on the effectiveness and scale of the cyber campaign in question. It should be noted that these support actions can be performed with the basic skills and resources defined above.

3.1 PROPAGANDA AND RECRUITMENT

Most contemporary conflicts are fought in the minds of the participants and the

spectators. In order to win, it is not necessary to kill every soldier in the opposing army or to raze the cities of the enemy. Instead, the participants compete to be *perceived* as the winning side. This is especially true in cyber conflicts, where permanent damage (physical damage, physical injury or death) is difficult to achieve. At the same time, the relative anonymity in the Internet causes attribution problems, which in turn make effective deterrence and retaliation nearly impossible. Therefore, in cyber conflicts it is very important to maintain the upper hand in the battle for the minds.

Creating a propaganda message requires no computer skills, while spreading it can be easily accomplished by e-mail, forum posts, etc. Therefore, a person can participate in an information operation or psychological operation (see Joint Publication 3-13) that supports the cyber campaign by affecting the morale of the participants (and spectators) and recruiting new members for the campaign.

3.2 SUPPLY

If one is not willing to participate in cyber attacks, one may still be interested in supplying the attackers. This may range from financial donations to corporate resource sharing.

Conceptually, one can find many ways to donate funds to a cyber militia. For example, a personal transaction (cash, wire transfer, check, etc.) is easy to accomplish, but it may leave a trail for the investigators and compromise the anonymity of the person. However, there are also alternative options, like donating stolen credit card information or channeling funds through on-line games and artificial worlds in cyberspace. It is also possible to offer personal resources, such as infecting one's computer with malware in order to add it to a botnet controlled by the militia.

Corporations and educational facilities tend to have much greater bandwidth and processing power than the average home user. Therefore, providing access (either physical access on site, or login credentials for remote access) to corporate resources can be very beneficial for the cyber militia.

3.3 TRAINING

A very useful way to contribute to a cyber militia is to provide training. This could range from posting simple attack instructions, such as the ping sequence described above, to a complicated real-time walkthrough of compromising a target system.

However, we have assumed the people in question to have no offensive skills, so

the training aspect would be limited to finding instructions on the web and posting them on the shared forum. This does illustrate, however, that the presence of even one expert can significantly affect the qualitative danger posed by the group.

3.4 RECONNAISSANCE & TARGETING

An important part in any offensive plan is to determine the right set of targets. This also holds true in cyberspace. It is very easy to cause collateral damage to systems that merely have a similar address or are located in the same IP address range with the intended target.

For example, let us assume that a conflict has erupted in a country that the attacker has little experience with. How does one determine which systems to attack if one does not understand the language used in the target country? Targeting everything within the country domain will spread the attack too thinly and may affect neutral and friendly systems in the area.

However, if there is someone in the group who knows the country in question, or at least can understand the language, he can help by pointing out which addresses should be targeted.

In addition, the group members can use dedicated tools to gather information about the configuration and vulnerabilities of the target system. It is important to note that these tools are not necessarily created for cyber attacks and may or may not be legal. Instead, they are often designed and used by security professionals who look for weaknesses in the system. For example, the attacker may use a vulnerability or port scanner software in order to identify potential avenues of attack for the group.

While scanning is not an attack, strictly speaking, it can be considered malicious, because the average Internet user should have no legitimate reason to do it. However, the information gained from the scan can then be forwarded to the more experienced attackers. This distracts the defenders, who will be aware of the scanner.

3.5 OBSERVATION AND FEEDBACK

Aside from providing targeting information, a “local” can also serve as an observer in the conflict and provide valuable feedback to the group. For example, if the group has organized a large-scale DDoS attack against a web server, it would be useful to verify that the system is inaccessible in the country or region of interest. The defenders could just drop all traffic coming from outside the region and continue to serve the local clients, so only a “local” can easily verify whether or not the system

is actually down.

Another observation function is to relay the effect on population to the attacking group. What are the locals talking about? Do they know who is responsible for the attack? Are they even aware of the attack? Has the local law enforcement or government made any statements in regard to the attacks? What effects does the attack have?

Having personal knowledge about the situation "in the field" can be very valuable for the people who are planning the cyber campaign. It can prevent "friendly fire" incidents, shift targets if the attack is unsuccessful, etc.

3.6 FOG OF WAR

Having the correct and up-to-date picture of the situation is important to all sides in any conflict. One way to exploit this is to inject confusing information to distract the attention and resources of the defenders.

For example, if the defenders rely on human reports (for lack of an automated reporting tool) for detecting successful attacks, then one could just generate false reports. The defenders will then have to waste precious time and resources to verify the information. Furthermore, if the "reporting" is public, then the "attack" will live on as a rumor even after proven false. One could also report fake events that are difficult to verify, such as counterattacks from the defenders ("they defaced several sites in country X as retaliation!"), temporary failure of critical services ("the 911 system was down for 20 minutes!"), some other group taking responsibility for the attacks, etc. This will reduce the situational awareness of the defenders.

In addition, one could provoke people to join the conflict on either side, as well as recruit support from third parties. Another option is to abuse the legal framework of the defenders to overload them with legitimate, but pointless, information queries (for example, requesting information that the target is required to provide, such as official contact information). In the end, there are many ways to make the fog of war thicker for the defenders, thus reducing their ability to effectively deal with the situation. As the examples demonstrate, these options do not require in-depth technical skills and can be easily performed by the cyber auxiliaries.

4. CONCLUSIONS

While the analysis has focused on the options available for untrained individuals, the examples from recent cyber conflicts clearly demonstrate that they do not work alone, but rather support the efforts of more skilled attackers. As a result, untrained individuals have successfully participated in cyber attacks that affect entire states, while there has been little or no direct attribution to any state or individual (Carr, 2009; Nazario, 2009).

There is no question that an unskilled attacker can find instructions on the web, but they are not likely to mount a successful attack against a well-defended system. The cyber attack categories reviewed here – DoS, DDoS, web defacement and malware attacks – are all accessible to persons with no prior experience. However, in most cases these attacks would not be severe enough to pose a serious threat in the international setting, because the untrained attackers can only use the most primitive attack forms.

In order to really be effective as a cyber militia, at least some of the members must have a deeper understanding of cyber attacks. While the "farmers with laptops" can carry out simple commands or run custom scripts and programs, someone still needs to provide them with the right tools, the correct instructions and point them against a reasonable target. This implies that defenders should focus their investigation and potential counter-actions against the cadre of instructors.

It is also clear that people, who are untrained in cyber attacks, can provide support to the experts, who can then focus on the cyber attacks. The main benefit of the support actions may be to create confusion for the defenders, because it is often useful to strike from chaos (fog of war) and keep the opposition guessing on your identity, aims and capabilities.

Of the examples provided, the most dangerous attack option is probably to implant malware into the target system in a time of crisis. The most influential support option, on the other hand, is to provide training and tools for the group. However, a person who wants to participate is not limited to just one option. Instead, active members of a (ad hoc) cyber militia can be expected to contribute in multiple ways, including both attack and support options.

5. SUMMARY

The (ad hoc) volunteer cyber militia groups have played a visible role in many recent international conflicts by waging a parallel campaign in cyberspace. While there seems to be evidence that most of the people engaged in this activity are untrained in the art of cyber war, they can still pose a threat if they are organized and "armed" by a more experienced *cadre*. Specifically, someone needs to provide them with attack instructions and software tools.

I have described some relatively simple ways to participate in cyber attacks, as well as to support others in doing so. Based on the described options, I have drawn conclusions on the danger posed by untrained cyber attackers.

REFERENCES

- Carr, J., 2009. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media.
- *Joint Publication 3-13.*, 2006. *Information Operations.* Chairman of the Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. [Accessed 25.02.2010]
- Nazario, J., 2009. Politically Motivated Denial of Service Attacks. In: Czosseck, C. & Geers, K. (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare,* Amsterdam: IOS Press, pp 163-181.
- Ottis, R., 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare and Security,* Plymouth. Reading: Academic Publishing Limited, pp 163-168.
- Ottis, R., 2009. Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. *Proceedings of the 8th European Conference on Information Warfare and Security,* Lisbon. Reading: Academic Publishing Limited, pp 177-182.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

GETTING THE ESSENCE OF CYBERSPACE; A THEORETICAL FRAMEWORK TO FACE CYBER ISSUES

Vincent JOUBERT[a1]

[a]*Raoul Dandurand Chair, Montréal, Québec, Canada*

Abstract: If a nation wants to be a great cyber power, it must elaborate a comprehensive national cyber strategy that will encompass the changes brought out by cyber capabilities and interconnected networks. This strategy must be conceived within a theoretical framework that defines the essential concepts of the cyber domain. To understand why this theoretical framework is vital to a nation's efficient cyber power, we will analyze the national strategy developed by the United States and the People's Republic of China and set the limits of each strategy.

An analysis of the military approach to the cyber domain of the two nations will show how these powers developed strong capacities and elaborated a holistic doctrine that allows the armies to wage Network Centric Warfare; after this statement, our analysis will lead us to consider the influence of the political and economic regimes on the securitization of the cyber domain.

The limits of the actual strategies will help us demonstrate that the cyber domain and its concept need to be clearly defined by the political, military, economic and academic spheres to provide a theoretical framework; such a framework, in the end, will help the governments adopting an efficient and comprehensive national cyber strategy that will serve the nation's interests and economy.

Keywords: Strategy, theoretical framework, cyberspace, United States, People's Republic of China, political regime.

1 Raoul Dandurand Chair of Strategic and Diplomatic Studies, 455 boul. René-Lévesque Est, UQAM, Pavillon Hubert Aquin, 4e étage, Bureau A-4410, Montréal (Québec) H2L 4Y2, CANADA. Email: vincent.joubert1@hotmail.fr.

INTRODUCTION

Cyber attacks are emerging as one of the types of new threats nations will have to face in future wars. Cyber conflicts are becoming part of more traditional conflicts, and digitalized nations have to elaborate a response plan to secure their networks and the nations' interests against the growing cyber threat. This response plan has to encompass every area affected by cyber conflicts, which pretty much represents all the most important sectors of modern societies as they all deeply rely on digital infrastructures and, therefore, face greater cyber attacks with strong consequences.

Because of its sole nature cyberspace cannot be controlled, even by an international organization such as NATO – the complexity of this man-made domain makes its dominance arguably impossible (Kramer, 2009). However, there are some steps government officials, military chiefs and policymakers must take to fully understand the issues and the consequences cyberspace and cyber conflicts have on international relations and modern societies, and try to regulate its use as well as secure their national networks.

One important step governments must take is the elaboration of a comprehensive national cyber strategy in which national interests would be protected and political objectives pursued. This strategy should provide a global evaluation of the environmental modifications cyberspace and cyber capabilities have created, and shall be derived from a theoretical framework that identifies the existing cyber concepts and from which the political objectives can be identified.

Such a theoretical framework is vital to understanding the cyber domain and developing relevant policies that will allow "digitalized" nations to secure their networks. Like all other new technologies, the cyber domain has created military strategy modifications that impact the global interactions between nations as it affects the very character of war (Cebrowski & Garstka, 1998). In this context, understanding the modifications of the threat perception and what security means in cyberspace will provide an answer on how to secure cyberspace. Because the goal for the governments is to secure their networks and build offensive and defensive cyber capacities, there has to be a theory that defines all the different concepts that exist and cohabit in the cyber domain: cyber attack, cyber threat, cyberwar, cyber crime, cyber espionage, and cyber conflict.

The theoretical framework has to conciliate diverging opinions and define the common vision nations have on the cyber domain and its concepts to provide a comprehensive analytical framework to the decision-makers.

This is a hard task because nations have different national interests and rules that drive their societies. The government must therefore conciliate numerous securities

interests in cyber security, a terrain in which multiple discourses and securities compete (Hansen & Nissenbaum, 2009, 8), and all the referent objects are intertwined.

To understand why a theoretical framework that defines the cyber concepts and their meaning for national cyber security strategies is vital, we will undertake an analysis of the United States' [US] and the People's Republic of China's [PRC] approaches regarding cyberspace.

We will first analyze the United States' cyber strategy by looking at its military doctrine and strategy on cyberspace, the internal organization, the government's role and implication. In a second part, we will proceed with that of the PRC; we will look at how Chinese military strategists have developed a modern doctrine which includes the cyber capabilities in their traditional military doctrine, and then see how the closed nature of the Chinese political regime has allowed the central government to maintain rigid control over China's national networks. The conclusion of this paper will emphasize the limits of both types of cyber security approaches; our former analysis will lead us to question the impact of the governmental regime's nature on national cyber strategies, and to demonstrate the need for a theoretical framework for cyberspace and cyber concepts in order to better understand and manage future cyber conflicts.

1. THE UNITED STATES' LOSS OF CONTROL

The cyber domain as we know it today is the technical development of an American invention which was designed to exchange knowledge through the US in a very short time. The scientists who created the ARPANET network back in 1969 did certainly not imagine the possibilities they initiated then.

As the technologies improved, the United States and the world discovered the power of computers and networking; today, modern societies – the US on top – relies deeply on digital infrastructures and networks, and faces the possibility of being under cyber attack. The United States may even be more at risk for they are the primary world power and therefore are the target of many opponents. For the last twenty years though, the United States has failed to devise a strategy that would enable the nation to counter the new cyber threat and protect the American interests.

1.1 AN IDEALISTIC VISION OF WAR

"Our assessments of conflict scenarios involving state adversaries pointed to the need for improved capabilities to counter threats in cyberspace—a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunications networks. Although it is a man-made domain, cyberspace is now as relevant a domain for [Department of Defense] DoD activities as the naturally occurring domains of land, sea, air, and space. There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communications networks and assured access to cyberspace" (*Quadrennial Defense Review Report*, 2010, [QDR report]).

This is how the Department of Defense qualifies the growing relation between the US army, modern conflicts and cyberspace. The presence of a section specifically dedicated to cyberspace in the QDR Report is quite significant and reveals the importance the highest ranked military officials give to this domain (William J. Lynn III, 2010). Both the inclusion of a section in the QDR report and the increasing budget attribution make it clear that the US government has decided to enhance its capacities that will provide the nation with appropriate network defense.

The growing attention given to cyberspace can easily be understood by a simple analysis of the current US military doctrine. As the QDR report determines and expresses the defense strategy of the United States and establishes a defense program for the next 20 years (US State Code, 2004), it provides the government with a comprehensive definition of US strategic objectives and identifies the threats the United States could face in the future. Since the 1990s, the importance given to the technology as a vital tool to improve the army's operations' efficiency has led to the concept of the Revolution in Military Affairs [RMA], which was defined in 1993 by M.J. Mazarr as fundamental progress in technology or in doctrine or in an organization that renders the actual way of waging war obsolete. The RMA concept was based on four major concepts that would lead the US army to rethink its organization and to give technology tremendous importance. Those concepts are: information dominance, disengaged combats, synergy, and civilianization of conflict. Like we said, technology development had a huge impact on the elaboration of the RMA doctrine; taken as a whole, the RMA encompasses three components: the technological component manifested by the development and the use of new Information Technologies, the organizational component manifested by the army's command jointness, and the conceptual component in which technology has given rise to a

major military concept, the Effect-Based Approach to Operations [EBAO]. The EBAO concept is seen as "a process for obtaining a desired strategic outcome or 'effect' on the enemy through the synergistic and cumulative application of the full range of military and non-military capabilities at all levels of conflict" where an effect is "the physical, functional, or psychological outcome, event or consequence that results from specific military or non-military actions" (USJFCOM, 2010). It basically analyzed battlefields as a system in which the US army defined the most sensitive points that would blind and deafen the adversary and therefore render him unable to wage war (Coquet, 2007).

Following the RMA logic, Donald D. Rumsfeld, then Secretary of Defense, began the US Army's *Transformation* in 2001; this transformation would modify the American army and forge the ideas that would allow the United States to face future threats, by deeply reorganizing the army's structure and focusing on technologies' use to win future conflicts. This technology-centered approach is very typical of American culture; US Army leaders have always considered technology as the key answer to new threats and have developed an almost religious-like trust in it (Henrotin, 2008).

The development of Information Technologies and the fast spread of the Internet network contributed to the rise of a new kind of warfare such as Information Operation [IO] and Network Centric Warfare [NCW]; as the essential component of the EBAO concept and a central component of the RMA, information itself became essential to control in order to win modern wars. Those wars are tightly linked with the capacity for the US Army to achieve full-spectrum dominance in its operations, and the relation between IO and cyberspace was made clear in Joint Publication 3-13 when defining IO as: "the integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception, and Operational Security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own". Some authors think it is erroneous to equate cyberspace with IO though; they rather view cyberspace as a critical aspect of the global information environment through which information operations are conducted, but not as the entire environment (Khuel, 2010; England, 2008).

Cyberspace and cyberwar offer unprecedented possibilities to military society, because modern societies rely deeply on networks and digital infrastructures, and moving warfare in cyberspace would give rise to new kinds of threats and new kinds of attacks. Cyberwar perfectly matches the idealistic RMA's vision of war in its possibility to wage a fast, long-distance and conclusive war with no casualties and little collateral damage (Henrotin, 2008).

Unfortunately, even if the networks are nowadays omnipresent the idealistic vision

of war as wanted in the RMA does not mirror the reality of conflicts. The technological answer NCW was supposed to provide to any kind of conflict faced the harsh reality of the vital importance of the human aspect of war (Wilson, 2007). The disillusions created by the tactical and strategic difficulties the US Army faced in the Afghanistani and Iraqi conflicts did not stop the army's organizational and doctrinal adaptations; both the Navy and the Air Force took action to improve their capabilities to operate in cyberspace, and the Army and the Marine Corps are also developing concepts and capabilities for cyber operations (Khuel, 2010). Cyberspace represents a new domain and strategists face the challenge to integrate its capabilities with other elements and instruments of power. Such can be achieved by drafting a national cyber strategy that would define the political objectives, be integrated in the broader national defense strategy, and which would be a strategy of partnership with all the actors present in cyberspace. This is precisely what the United States has failed to do.

1.2 A POLITICAL AND ECONOMIC EXPLANATION OF THE FAILURES

Nearly every day the United States is discovering new threats and attacks against the country's networks. Inadequate cyber security and loss of valuable data have inflicted considerable damage to US national security (CSIS, 2008).

Over the last two decades, the presidential administrations have recognized the strategic importance of cyberspace; governmental measures like the *Presidential Decision Directive/NSC-63* (Clinton administration, 1998) and *The National Strategy to Secure Cyberspace* (The White House, 2003) have been taken to maintain the US's competitiveness in this domain, yet the latest officials' reports reveal a real problem of coordination between federal agencies that are in charge of the US networks' security (GAO-10-338, 2010; McAfee report, 2009). Several simulation exercises were made to evaluate the US cyber defense capabilities such as Cyberstorm I & II, and as for now, the results point out a worrying absence of coordination, task appointment and clear hierarchy between federal agencies (GAO-08-825, 2008). When writing this paper at the very beginning of 2010, there were eight agencies in charge of protecting and defending US networks and vital digital infrastructures; global US networks cannot be efficiently managed if those agencies have overlapping and uncoordinated responsibilities for cyber security. The bureaucratic disputes that can occur between some agencies will also increase delay and inefficiency in the response to a cyber attack and will be damageable to the whole US network (Halperin, Clapp, 2006). Following the 60 Days Cyber Policy Review's recommendations, Barack Obama appointed Howard A. Schmidt New Cyber Coordinator last December; this is a first step in improving the coordination and the collaboration between

those agencies, hence reducing the vulnerabilities on the networks and improving cyber security. Disorganized federal management of cyber attacks is truly harmful to the US networks' security and can be modified with a clear and holistic mission order established by the White House.

Securing the US's critical digital infrastructures cannot be done only by federal agencies though, for the majority of the network is designed, owned and used by private companies. Private sector interests and national security challenges are therefore intertwined in the cyber domain and the government has to find the right balance to involve these companies in building strong cyber defenses without creating obstacles to their business. The public and the private sectors have different objectives and different budget management, and where the public sector will spend more money on securing the networks to avoid intrusions or attacks, the private sector will be more likely to think in terms of profits and business expansion at the expense of security improvement (Cyber Policy Review, 2009).

There is little doubt that cyberwarfare will have a significant impact on the private sector, but the roles and responsibilities remain unclear in case of a conflict and neither the government nor the private sector will benefit from this situation. Companies that design and produce software will have to play a role in cyber security, but the limits of their responsibility and the exact nature of their role in detection and response are not specified and nobody can provide an answer on that specific point (McAfee, 2009).

The recent cyber incidents show that deregulation has proven its inability to create a safe and secured cyber environment because self-regulation obviously did not work.

The absence of regulation in today's cyberspace represents a great danger to cyber security. The intellectual heritage of deregulation of the last administration leaves a continuing feeling that regulation is an obstacle to free-market economics and innovation and is not a solution to improving cyber security. Some comparisons with other regulated areas aim to prove that regulation is a danger for innovation and not the key to a secure cyberspace. The key argument of deregulation partisans is that regulation will impose certain standards and forbid experimentations, which is a vital aspect of competitiveness and free-market economics (Harper, 2009; Lewis, 2009). The pro-regulation answer is that regulation is not always bad for development of the market and innovation in a society where security and safe products are highly demanded. Therefore it would be adequate to ask private companies for more security standards in the cyber products and services they provide, and the companies could manage to find in security competitiveness new market opportunities. Regulation must not be overly prescriptive, but looking at the actual cyber environment, regulation will be better than no regulation at all (Lewis, 2009).

Here the US government faces a problem that is directly linked to the economic regime of the country; the economic principles that drive the American market emphasize individual freedom and market freedom and free enterprise that have not precluded a major role for the government (United States Information Agency, 1992). However, the threats created by cyberspace might affect the whole of US security and the economy if the *status quo* is maintained. The government will have to work in close collaboration with the private sector to find a solution that won't affect those pillars of American state power.

Another problem that inhibits efficient collaboration between the public and the private sectors is about privacy points; this concern tends to restrain the private sector from automatically sharing information with the federal agencies to strengthen security on their networks. Industry has also expressed reservations about disclosing to the Federal government sensitive or proprietary business information, such as vulnerabilities and data or network breaches (Cyber Policy Review, 2009). The private sector believes that sharing a vulnerability with the government authorities might expose their company to potential economic disadvantage, for their customers would not trust the company and therefore deal with the competitor. A vulnerability disclosure would financially affect their business so the company will try to manage the problem alone, hiding the attack and not alerting the authorities.

The government must take a strong decision to conceal those concerns and tighten private-public sector collaboration. An efficiently secured global network cannot be possible without it. China, on the other hand, does not face such a problem.

2. THE PEOPLE'S REPUBLIC OF CHINA'S INFORMATION WARFARE STRATEGY

The People's Republic of China (PRC) developed an Information Warfare (IW) strategy a decade ago to leapfrog the technological-military delay they had *vis-à-vis* the United States. When looking at the PRC's actual cyber capabilities, you can easily come to the conclusion that the strategy they elaborated and established was a success.

2.1 CHINESE MILITARY STRATEGY THINKING

The Chinese strategic mind-set differs markedly from that of the US. The People's Liberation Army's (PLA) officers and military strategists have developed specific concepts that guide the strategic choices of the PRC and that led the PLA to conduct its own Revolution in Military Affairs.

Even though the Chinese don't use the word cyber in their lexicon to qualify the new technologies and rather talk about *informatization*, one must not be misled here; they are talking about cyber capabilities and cyberspace to wage information warfare (Thomas, 2009).

An ongoing critic of the Chinese military doctrine regarding information warfare is that it is not really a Chinese doctrine; the literature on this subject describes the strong similarities of the Chinese Information Warfare strategy with that of America (Mulvenon, 1999). Ten years ago, some of the most respectable American researchers stated that the PLA did not have a coherent information warfare doctrine, nothing compared to the US's writings on the subject, and that even though the PLA's capabilities were growing, they did not match their strategies. Since then, opinions have changed as the PLA developed a coherent doctrine and the matching capabilities (Gertz, 2009).

Two of the most important and influential Chinese military strategists, Li Bingyan and Dai Qingmin, characterized the modifications cyber capabilities brought to modern conflicts. They both agree on the fact that the perception of war has changed and that the strategy must therefore be adapted to these changes; Chinese military strategy should absorb new methodologies such as cybernetics and information theories but also integrate them to ancient military stratagems. A new strategy that includes cyber capabilities will also give the PRC the opportunity to use asymmetric means against more powerful nations such as the United States (Li, 2004; Dai, 2002). In other words, cyberspace gives new tools to the PRC that they can use to improve their military assets and capabilities that could eventually challenge greater nations.

One of the most important writings that had a huge impact on the PLA's approach to new types of conflicts created by new technologies, *The Science of Military Strategy*, written and published in 2001 by Peng Guangqian and Yao Youzhi, two major PLA's generals, elaborated strategic analyses and offered a holistic definition of the modern Chinese strategy.

The main point discussed in the book that defines the broader concept of the Chinese strategy is the Science of Strategy (SOS); the US has not yet defined this concept but the authors see it as a military science characterized by politics, antagonism, comprehensiveness, stratagem, practice and prediction (Thomas, 2007).

A detailed analysis of *The Science of Military Strategy* made by Lieutenant Colonel Timothy L. Thomas (2007) reveals the major differences between the Chinese and the Western strategies and makes it clear that Peng and Yao's work provides a deep theoretical analysis of the Chinese strategy. Thomas describes how the SOS is divided into two categories, the basic theory of strategy and the applied theory of

strategy which both contribute to the elaboration of the broader concept of the PLA's military strategy using its cultural legacy and incorporating technology to fight future wars. Those elements reveal the essence of the Chinese strategic elements and therefore give us a good comprehension of their strategic mind-set (Thomas, 2007).

"Chinese military planners studied the high-tech experiences of US forces to examine the effects of information technology on military strategy and future warfare" says Thomas, and they came to the conclusion that war and strategy "have never been changed so dramatically and profoundly" (Thomas, 2007, p. 54). Peng and Yao even say that dramatic developments in the practice of wars urgently require new theoretical explanations about the emerging situation (Peng and Yao, 2001).

In 2007, the *China National Defense News* defined cyberwarfare as a "struggle between opposing sides making use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology". Cyberwarfare is an important means of achieving control of networks, which is a vital aspect of China's information operations' theory. Control of networks requires broad reconnaissance and espionage activities during peacetime to know the enemy and to provide the Chinese with the possibility of preemptive attacks. The emphasis on an active offense is one of the most important points on which the Chinese strategists insist for they consider a defense-only attitude to be irrelevant in information warfare. This is also a major shift in the Chinese military doctrine for they traditionally adopt a strategy of active defense and it shows that Chinese strategists have found a new scope for the PLA's operations in information warfare (Thomas, 2009).

Chinese strategists have theorized the transformation of modern conflicts by analyzing the new capabilities involved and the impact they had on warfare. Consequently, they adapted the Chinese military strategy to those changes by incorporating new technologies to ancient stratagems. Where US strategists seek a technological solution, the Chinese rather use stratagems and strategic sophistications. The Chinese strategy hence gives us a very interesting approach to cyberspace and indicates that theoretical work is an essential step for an efficient military doctrine that will provide the army with a holistic understanding of cyberspace.

2.2 A GOVERNMENTAL CIVIL STRATEGY

The PRC's officials have long considered the Internet and information technologies as a lever to the PRC's economic modernization and as a tool to maintaining its international competitiveness. They assumed they needed to integrate the information and communications technologies to Chinese society and started an *informatization* process back in the 1990s (Foster & Goodman, 2000).

This process was established by the central government and was part of a broader strategy to develop a knowledge-based economy, which relied on a series of "Golden Projects". The main objective of those projects was to build a national information network that would facilitate the economic modernization of the PRC, develop information and communications technologies, and interconnect the PRC's states to allow better interaction and control of the central government upon the other departments (China Internet Network Information Center, 2006).

This vast project was divided in three stages that would progressively build the national PRC's cyber capacity. The first stage was the establishment of physical infrastructures and digitalization of information in databases to provide the central government with knowledge of international commercial transactions and the ability to communicate with the Party's officials; the second stage centered its improvements on the PRC's economic and financial areas and education, and the last stage focused on the other economic areas that were not digitalized – enterprise, agriculture, health, information, housing, and manufacturing of communications devices (Lovelock & Ure, 2002).

The establishment of an "e-government" reveals the proactive Internet management strategy of the central government where they use the Internet as a lever to modernize and develop the national economy and keep international competitiveness but also as a tool to promote the Party's ideas, to fight existing corruption and to interact with the population (Foster & Goodman, 2000).

A plan such as the Golden Projects is part of the broader national cyber strategy to set up control over the national networks. The different Party leaders took the necessary steps to establish a governmental strategy that would modernize Chinese society and lead the nation to become one of the most influential in cyberspace.

The Golden Projects allowed the PRC to become the nation with the most Internet users today and one of the most active in terms of cyber capabilities' use. The nation continues to develop its networks through plans that will bring information and communication across the whole country (CINIC report, 2009); even though the technical challenge is great, this interconnectivity development follows the strategy established by the central government and will be used as a way of controlling the population.

The PRC has released in 2006 the *2006-2020 State Informatization Development Strategy* in which it set forth China's goals in informatization development for a 15-year period. Among those objectives, the PRC is willing to become independent in innovation of information technology in order to boost the research and development as well as the manufacturing sectors, and the strategy also emphasizes orienting the national economy and society toward information to develop those sectors; it

also calls for a national information security system that would provide security and control of the networks. The PRC has already begun doing so with the Kylin exploitation system, which provides high-level security to the Chinese Internet network.

This cyber strategy established by the PRC aims to promote social and economic development through informatization development of the entire nation. The PRC clearly wishes to use cyber capabilities as a lever to meet the challenges and grasp the opportunities arising in the economic, military, social and scientific areas. The central government maintains its control over the networks by imposing strict rules and regulations to the foreign companies that come and settle in China so that it does not lose control over the population (US-China Economic and Security Review Report, 2009).

To date, China has succeeded in building an advanced digitalized society that would improve its economic profits and its society's access to information and communications technologies while modeling this connected nation within the Party's ideas and guidelines.

The military theoretical works provided by the most influent strategists and the establishment of a national cyber strategy allowed the PRC to fully integrate cyberspace and its capabilities in Chinese society.

As a result of this, China is quite arguably the greatest opponent to the United States in cyberspace; it is not yet an enemy, but the recent events involving US firms and the allegations of Chinese governmental intrusions only tend to tense the relations. Moreover, the PRC is making significant moves to tie its cyber capabilities to its strategic concepts and is taking a more active posture than that of the United States (Thomas, 2009).

3. CONCLUSION

The United States and the People's Republic of China are two nations that are competing in cyberspace, testing their technologies and their strategies against each other's networks.

To better understand their vision of cyberspace and how the governments apprehend the cyber issues arisen from the growing cyber capabilities, an analysis of each national strategy is necessary. We have seen that both countries have adapted their military doctrine to this new strategic domain to ensure that they have the capacities to conduct network-centric warfare; the United States focuses on technology where the PLA will include ancient Chinese stratagems to the existing technologies.

A military strategy alone is not sufficient to acquire a holistic understanding of cyber concepts though; modifying the national military strategies to adapt it to the modifications the cyber domain created is an essential step but not an end. The obvious reason for which a military solution alone is irrelevant in cyberspace is because cyberspace is not confined to the military sphere – it reaches every sector of modern societies.

The civil sphere is using cyberspace at least as much as the military; the entire globalized economy relies on cyberspace and every digitalized nation has "computerized" its vital infrastructure. The direct consequence of this strong dependence is that the government has to provide cyber security to the whole nation to protect its national and economic interests.

The United States and China have very different approaches to securitizing their national networks. The difference resides in the political and economic regimes of those nations, which define the government implication in control and protecting the networks and digital infrastructures of the country.

The Chinese Communist regime gives the central government the capacities to control and conduct repression measures on the party's dissidents. Because of this strict control on the Internet and infrastructures as well as on innovation and development programs, Chinese information technology and networks look safer than other networks in other countries; but the security those networks enjoy is closer to censorship than to an effective securitization of cyberspace. Chinese networks face the same types of attacks as the US, and security in Chinese cyberspace may not be this elevated.

The democratic regime and liberal economy of the United States have allowed the country to develop a strong economy and design high technologies that are the structural elements of cyberspace, but because the vast majority of the networks is owned by private companies the government cannot impose arbitrary regulations; the problem here is to balance the privacy rights owned by the private sector – market freedom, information privacy – with the security vulnerabilities that threaten the national power. A closer collaboration with the private partners associated with a privacy guarantee would benefit both the private and public sectors.

This collaboration has to be completed with an essential step; there is no consensus on those notions that are the fundamental concepts defining cyber threats today; this will inevitably lead the policies to failure. No single national strategy will be efficient until the expectations on these fundamental security concepts are clearly defined. To provide a better understanding of cyberspace and cyber threats, the nations must elaborate a theoretical framework in which the essential concepts are analyzed and explained to the decision-makers.

The multiplicity of actors in cyberspace creates complex interactions and expectations that are not necessarily the same, diverging from one actor/referent object to another. The first step is the appropriation of the military strategic modifications arisen from the new capabilities created by cyberspace, which we find in both the US and Chinese military doctrines. Once these new capabilities have been fully understood, the government must define the meaning of the new security and strategic issues created, which are here the main cyber concepts: cyber threats, cyber security, cyber espionage, cyber attack, and cyberwar. Theorizing the cyber domain requires identifying the actors that are the referent objects, and linking the different security discourses to provide a securitization framework (Hansen & Nissembaum, 2009).

The semantic appropriation is also essential to clearly define thresholds and avoid any undesired escalation of violence. Once the government has adopted definitions of cyber concepts, it should integrate these notions in a comprehensive national cyber strategy, in which it will work with the appropriate actors to meet the political objectives it defined in the earlier step. The elaboration of such a theoretical framework is absolutely vital for better appropriation of the cyber domain.

REFERENCES

- Cebrowski, A. & Garstka J., 1998. *Network-Centric Warfare: Its Origin and Future*. Proceedings, pp. 28-36.
- Center for Strategic and International Studies, 2008. *Securing Cyberspace for the 44th Presidency.* A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington D.C.
- China Internet Network Information Center (CINIC), 2009. *Statistical Report on Internet Development in China.*
- Coquet, P., 2007. « Opérations basées sur les effets : rationalité et réalité », *Focus Stratégique No 1*, Laboratoire de Recherche et de Défense, IFRI, Paris.
- Dai Q., 2002. "Discourse on Armed Forces Informationization Building and Information Warfare Building," in *China Military Science, 2002.*
- Department of Defense, *2010 Quadrennial Defense Review Report,* Department of Defense, Washington D.C
- England G., 2008. Deputy Secretary of Defense Memorandum to the Military Departments et al., "The Definition of Cyberspace", Washington D.C.
- Foster W. & Goodman S., 2000. *The Diffusion of the Internet in China*, Center for International Security and Cooperation (CISAC), Stanford University
- Gertz, Bill, 2009. China blocks U.S. from cyber warfare. *The Washington Post.*
- Guangqian, Peng, & Youzhi, Yao eds., 2001. *The Science of Military Strategy*, English version (China: Military Science Publishing House, Academy of Military Science of the Chinese People's Liberation Army, 2001).
- Hansen, Lene & Nissenbaum, Helen, 2009. "Digital disaster, cyber security, and the Copenhagen school", *International Studies Quarterly*, vol. 53, 2009, pp.1155-1175.
- Harper, Jim, 2009. *"Government-run cyber security? No thanks"*, CATO institute, TechKnowledge.com, 13 march 2009, available: http://www.cato.org/tech/tk/090313-tk.html [February 14th, 2010].
- Henrotin, J., 2008. *"La technologie militaire en question – Le cas américain"*, Paris, éd. Economica, Coll. Stratégies & Doctrines.
- Khuel D., 2009. "From Cyberspace to Cyberpower: Defining the Problem", in F.D. Kramer, S.H. Starr, and L.K. Wentz (Ed), *Cyberpower and National Security*, (pp.24-42). Washington D.C, USA : Potomac Books, Inc. 2009
- Kramer, Franklin, Starr, Stuart, & Wentz, Larry, 2009. *Cyberpower and National Security*, Ed. Washington D.C.: Potomac Books.
- Lewis, James, 2009. « Innovation and Cybersecurity Regulation », Washington D.C: Center for Strategic and International Studies, May 2009, available: http://csis.org/files/media/csis/pubs/090327_lewis_innovation_cybersecurity.pdf [February 14th, 2010].
- Li B., 2004. "Applying Military Strategy in the Age of the New Revolution in Military Affairs," in *The Chinese Revolution in Military Affairs*, ed. Shen Weiguang (Beijing: New China Press), 2-31.
- Lovelock P. and Ure J., 2002. "E-government in China", pre-publication version of the chapter to appear in Zhang Junhua, Martin Woesler, eds. *China's Digital Dream – the Impact of the Internet on the Chinese Society*, the University Press Bochum
- McAfee Virtual Criminology Report 2009: "Virtually Here, The Age of Cyber Warfare", Santa Clara, CA.
- Mulvenon, James, 1999. "The PLA and information warfare", in *The PLA in the Information Age,* James C. Mulvenon & Richard H. Yang, Santa Monica, USA: RAND cop, pp.175-186.
- Office of the Law Revision Councel, 2004. *United States Code, Titre 10, Section 118*, Washington D.C.
- The White House, 2009. *Cyberspace Policy Review, Assuring a trusted and resilient information and communications infrastructure*, Washington D.C.
- The White House, 2003. *The National Strategy to Secure Cyberspace*, Washington D.C.

- Thomas T., 2009. "Nation-state Cyber Strategies: Examples from China and Russia", in F.D. Kramer, S.H. Starr, and L.K. Wentz (Ed), *Cyberpower and National Security*, (pp.465-488). Washington D.C, USA : Potomac Books, Inc.
- Thomas, Timothy L., 2007. "The Chinese Military's Strategic Mind-Set", *Military Review*, November-December 2007, pp.47-55.
- United States Government Accountability Office (GAO), 2008. Report to Congressional Requesters, *"Critical Infrastructure Protection, DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise"*, Washington D.C
- United States Government Accountability Office (GAO), 2010. *"Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative"*, Washington D.C.
- United States Information Agency, 1992. *An Outline of the American Economy,* Washington D.C.
- US Joint Forces Command, definition available at http://www.jfcom.mil/index.htm [March 25th, 2010].
- US-China Economic and Security Review Commission, *2009 US-China Economic and Security Review Report,* Washington D.C.: 2009.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

KNOWLEDGE BASED FRAMEWORK FOR CYBER WEAPONS AND CONFLICT

Peeter LORENTS and Rain OTTIS

CCD COE, Tallinn, Estonia

Abstract: In recent years there have been a number of international conflicts that have been mirrored by a parallel campaign of hostile actions in cyberspace. This, in turn, has prompted various attempts to analyze the phenomenon and explain the threat to the wider public. Unfortunately, however, the reports and analysis are often confusing and can include rather arbitrary use of various cyber "buzz words". It follows that there is a need for a formal rigorous model for describing and analyzing cyber conflicts. Formal methods are also necessary for developing artificial intelligence-enabled offensive and defensive systems for cyber conflicts.

In order to provide a remedy for this issue, we propose a formalized framework of key terms in cyber conflict. We begin by revisiting the concepts of knowledge, data and information. Based on that we proceed to define "information system" and "intelligent system". We provide a formal description for the concept of destroying and falsifying information and explain the concepts of confidentiality, integrity and availability as part of our framework. We then propose definitions for cyber weapons, cyber incidents, cyber attacks, cyber espionage, cyber conflicts and finally, cyberwar.

The framework is based on formal logic and allows for theoretical, experimental or empirical research with mathematically provable results. As such, it can provide a solid backbone for cyber conflict research, which is often based on less rigorous methods.

Keywords: knowledge, data, definitions, cyber weapon, cyber conflict

INTRODUCTION

Threats from cyberspace differ from most traditional threats, because they are global, often unpredictable and can affect our lives when we least expect them. For example, a political dispute between two countries can unleash a wave of cyber attacks, which take down an international bank, causing discomfort and economic damage in countries unrelated to the conflict. A war on another continent does not pose a threat to the average citizen, but a cyber campaign anywhere in the world can potentially reach us in our homes.

Over the past few years the public perception of the threat from cyber attacks has risen considerably. Therefore, it is important to analyze the phenomenon in a systematic and scientific way. To achieve this, we must either choose or create an applicable terminology and scientific methods, which allow theoretical, experimental and empirical studies with reliable results.

In order to effectively handle events in cyberspace, we (humans) first need to be able to clearly describe these situations and events, and any constraints that apply to them. Based on this we need to derive an appropriate decision for dealing with the situation. The events in cyberspace surpass the human ability to comprehend them, both in terms of the amount of available information, as well as the speed of the changes that take place in cyberspace. One way to manage this problem is to enlist computers to provide decision assistance or even fully automated decisions. This, however, requires that we use a framework that is compatible with the formal logic of the computer. In order to satisfy this requirement, we present a framework (described below) that is based on formal mathematical theories (proof theory, model theory, algebraic systems theory, etc.).

This is the only way to *really* provide a framework which is applicable for both human decision-makers and automated decision support systems, and that is based on a (A) reliable, (B) credible and (C) commonly agreed foundation and that (D) works. The framework can, in turn, be used to:

- adequately explain past, present and potential future cyber events to the public and decision-makers,
- develop means to monitor the situation, assess the threats, as well as provide necessary security and preventive actions,
- create applicable regulations, laws and international treaties.

Unfortunately, there is still no common and general set of exact science and engineering terms that covers the basic concepts of information and communication technology. In other words, there are no commonly agreed terms that would al-

low formulating arguments and strong proofs of these arguments. For example, the concepts of *knowledge, data* and *information* (not to be confused with the practical measure of information I, which can be found using Hartley's (1928) formula $I=\log_a m^n$).

In this work we focus on understanding terms that are related to information, operating with information and the problems associated with information, including confidentiality, availability and integrity. We finish with the concepts of cyber weapon, cyber incident, cyber attack, cyber espionage, cyber conflict, and cyberwar. We provide definitions on these various concepts, based on the definitions of knowledge, data and information that were developed by Lorents (Lorents, 2001, 2008; Lorents, Ottis, & Rikk, 2009).

1. KNOWLEDGE, DATA AND INFORMATION

In order to explain the concept of information we use the definitions of knowledge and data. These definitions are based on the binary relation between such pairs, where the first object is the symbol, sign, name, etc. (notation), of the second object, which, in turn, is the meaning (denotation) of the first object. It is important to note that the notations and denotations are not limited to only things that can be seen or heard by humans (for example, gestures, signs, symbols, texts, pictures, etc.).

Let us agree that if A is the notation for B and, at the same time, B is the denotation of A, then we can represent this relationship as $(A \int B)$, or in simple cases as $A \int B$. The symbol "$\int$" represents a stylized letter S (referring to words like "signum", "sign", etc.). Let us also agree that if we have formed an ordered pair, where A is the first element and B is the second element, then we represent it as $\langle A,B \rangle$.

Note that the notation-denotation relationship "$\int$" is a fundamental relationship, and therefore it has no definition. This, however, does not mean that we cannot formulate the properties of this relationship. These properties can be represented formally, so they can be considered as logic formulas. There are two types of assertions or arguments (expressed by logic formulas). The first type is considered a priori proven – axioms or postulates that serve as the foundation. The second type consists of all the arguments that can be proven based on previously proven (including a priori proven) arguments.

The properties of the notation-denotation relationship include, but are not limited to:

- *non-uniqueness* (Lorents, 2001). This means that there could be many denotations for a given notation, or many notations for a given denotation. For exam-

ple, (I ∫ "Roman number") and (I ∫ "capital letter i"), or (2 ∫ "two") and (II ∫ "two").

- *transitivity* (Lorents, 2001). This refers to the property that allows relationships to be "carried over", or in short (A ∫ B)&(B ∫ C)→(A ∫ C).
- *equality (*Lorents, 2005). If two elements are equal (same), then the first element can be used as the notation for the second element, or in short (A=B→(A ∫ B)). Note that while some things may seem obvious to a human, they still need to be either postulated or proven, in order to consider them correct. For example, it seems that if A=B, then both can be used as notations or denotations for the other. However, this still needs to be proven.

Proof for [X=Y→(X∫Y)&(Y∫X)]:

$$\dfrac{\dfrac{}{X=Y\rightarrow Y=X}\qquad \dfrac{}{Y=X\rightarrow (Y\int X)}}{X=Y\rightarrow (X\int Y)}\qquad \dfrac{}{X=Y\rightarrow (Y\int X)}$$

$$X=Y\rightarrow (X\int Y)\,\&\,(Y\int X)$$

Definition 1. If some objects A and B have the relationship (A ∫ B), then the ordered pair ⟨A,B⟩ is called knowledge (Lorents, 2001, 2008).

Therefore, if some objects A and B have the relationship (A ∫ B), we can say that the denotation (meaning) of A is *known*. Similarly, we can say that the notation (symbol, sign etc.) of B is *known*.

Note that knowledge is an ordered pair of some notation and its denotation, not the text (A ∫ B), which represents the *argument* that A and B have the relationship "∫". At the same time, not every ordered pair is knowledge, even if the elements in it are considered notation and denotation. For example, the ordered pairs ⟨II,2⟩ and ⟨V,5⟩ are knowledge (about the correspondence between Roman and Arabic numbers), but the ordered pair ⟨II,5⟩ is not (in this setting).

Definition 2. D is *data,* if there is an A, so that ⟨A,D⟩ is knowledge or if there is a B, so that ⟨D,B⟩ is knowledge.

From this definition, it follows that only an element (notation or denotation) from some piece of knowledge can be data. For example, data about European countries: there is data that Albania, Andorra, ⋯, and the Vatican are European countries.

Definition 3. Information is either knowledge or data (Lorents et al, 2009).

There are two implications from this definition:

1. something can be information only if it is knowledge or it has a notation or it has a denotation, and

2. if something is not knowledge, notation or denotation, then it is not information.

2. SYSTEMS, INFORMATION SYSTEMS AND INTELLIGENT SYSTEMS

It is possible to operate (for example, input, create, modify, store, systematize, output, transmit, erase, etc.) with information as states or changes of states (in case of time-dependent systems) of systems. By systems we mean a structured set of elements, or more precisely, for a system we need some fixed set of elements (basic set) and a fixed set of properties or relations of these elements (signature) (Cohn, 1965; Grätzer, 2008; Lorents, 2006; Maltsev, 1970). Note that it is *not required* to fix both properties and relations, nor is it required to fix all properties or all relations of the set of elements.

Definition 4. An *information system* is a system (a fixed set of elements and their properties or relations) that is designed to operate with information.

In simpler cases, where the only role of the system (or an object) is to store, present, etc., (to be in the role of a notation or denotation) information, we can say that the system or object *contains information, carries information, possesses information*, etc.

Definition 5. An *intelligent system* is a system that operates with knowledge (Lorents & Lorents, 2003; Lorents, 2008).

An important implication from this definition is that not every information system is an intelligent system. The defining characteristic of an intelligent system is its ability to operate with knowledge. Therefore, the mere presence of knowledge in a system does not automatically mean that the system is intelligent. A printed encyclopedia, for example, only contains information, but does not operate with it, so it is not an intelligent system.

Note that *it does not follow* from the information and intelligent system definitions, that a system which inputs and outputs only data is a "non-intelligent" information system. For example, processing (numeric) input data to get (numeric) output data often requires operations with corresponding knowledge.

Information systems, both man-made technological systems and the humans them-

selves, can be combined into "systems of information systems", such as cyberspace and cyber society (Lorents et al, 2009; Ottis & Lorents, 2010). Note that the term "cyber" has made a strong comeback after a few decades of relative quiet and regained its standing next to various "info"-related concepts. For example, cyber attacks, cyber defense, cyber weapons, cyber conflicts and cyberwarfare. One way to explain it is that we have witnessed an increased interest in incidents affecting the communication and control of systems that provide the everyday services of modern society. Communication and control, however, characterize the research field of cybernetics, which is the origin of the term "cyber" (Wiener, 1948).

In order to clearly describe and analyze events, it is important that these concepts can also be defined based on a steady foundation of basic terms and principles. This is especially important, if we want to use artificial intelligence to generate correct decisions from a correct description of the situation (which often requires an educated decision that is beyond the capability of the human, in terms of speed, memory, etc.).

3. SECURITY OF INFORMATION

Next we review the three security aspects of information systems – availability, integrity and confidentiality. Depending on the case the emphasis between these aspects may be different. For example, owners of a public news website are mostly concerned with availability and integrity of the displayed information, and not at all interested in maintaining the confidentiality of news stories. On the other hand, the list of double agents in an intelligence agency must be kept confidential, with secondary considerations for integrity and availability.

We also review two special cases of compromising the security of information – destruction and falsification of information.

3.1 AVAILABILITY OF INFORMATION

In the definition for information systems we stated that the system must be able to operate with information. However, in some cases the system may not be able to fulfill this requirement. There are two potential reasons for this:

1. The information that is required to complete the operation is damaged to the point where the system cannot function correctly. For example, a form of malware, called "ransomware", encrypts the files on the victim's system, rendering the system useless (as the victim can no longer access her information) until the owner pays a ransom.

2. The means to complete the operation are damaged or degraded to the point where the system cannot function correctly. For example, a piece of code could have a "memory leak", writing garbage data on the computer's memory until the performance of the system begins to degrade.

Remark. In principle, attacks against availability aim to deny the use or the designed functionality of the target system or information.

The "scientific inspiration" for hindering the transfer of information comes from Shannon (1949) and Tuller (1949). Their work gave us the formula for calculating the throughput capacity of an information channel: $W{\cdot}log_2(1+P/N)$, where W is the available bandwidth, P is the average power of the signal and N is the average power of the noise in the channel.

This, in turn, has led us to the estimation of the maximum information transfer rate: $K£W{\cdot}log_2(1+P/N)$ (Lorents, 2001b). Therefore, if we increase the power of noise in the channel, we will decrease the information throughput. This principle is applicable for all manner of "jammers", regardless of technical details. For example, it explains the availability issues resulting from a distributed denial of service attack or a simple e-mail spam flood.

3.2 INTEGRITY OF INFORMATION

In many cases we need to accept the fact that if even one element in a set is added, removed or replaced, then we no longer have the *same* set. This also applies to systems, where in addition to elements we need to worry about the properties or relations of the elements. In case of strictly formalized systems (Grätzer, 2008; Lorents, 2001b, 2006; Maltsev, 1970) the system is considered different even if only one property or relation of an element is added, removed or replaced.

This may not be a problem for a human, but it will affect the decisions of a *correctly* working artificial intelligence system. Therefore, we should discuss damaging or corrupting the integrity of information. Let us agree that:

- the *integrity of information is not compromised* if all (and nothing else) elements, their properties and relations are present *as they are meant to be* (for example, as they are fixed in a design document), and
- in all other cases, the *integrity of information is compromised* (destroyed, corrupted, damaged, etc.)

Remark. In principle, attacks against integrity aim to damage the structure of the target system or information.

Note that one way to corrupt the integrity of information (or destroy it) is to break the notation-denotation relationship (knowledge). Therefore, it is not always necessary to erase or corrupt data.

3.3 CONFIDENTIALITY OF INFORMATION

The confidentiality of information and the concept of secret information rest on the concept of knowledge. In addition, the time when some information must be kept confidential is also important.

Definition 6. Information X, A or B (where $X=\langle A,B\rangle$ and $A \int B$) is *confidential* from system S if system S *cannot be able to acquire* knowledge X during the designated time period (from t_0 to t_1).

Note that in this case it is the fact of (not) acquiring the knowledge that is important. It is also important to pick the time t_1 in such a way that there are no problems if the confidentiality is lost after t_1. For example, the detailed agenda and travel route of a visiting dignitary may need to be confidential (for personal security reasons) until he leaves. After that, the details can be released to the public.

When compared to the destruction of information, we see that instead of removing knowledge (X), notation (A), denotation (B) or the relationship between them ($A \int B$), we need to make it impossible for system S to possess and use (to reconstruct knowledge) them.

3.4 FALSIFYING INFORMATION

Falsifying refers to the process of making some information false. As a result, the integrity and availability of the original information is lost. In order to discuss the concept of falsifying information we need to review some basic terms. First, the concepts of "true" and "false" are in essence assessments. Assigning and using assessments requires answers to three simple questions (Lorents, 2006):

- What objects are assessed?
- What are used as assessments?
- How are assessments assigned to the assessed objects?

Let us agree that we want to assess logic formulas – objects representing arguments and constructed in a highly formal way. Note that the choice and assignment of logical assessments or truth-values is dependent on the underlying logic. For example, in the classical logic, we can use the binary Boolean logic elements (0

and 1), whereas in quantum mechanics we can use three truth-values (Birkhoff & von Neumann, 1936). Non-traditional logic frameworks (with more than two truth-values) are not only theoretical, but can be applied in various practical tasks, such as automatic synthesis of computer programs (Tyugu, 1988, 2007). Note that in case of non-traditional logic frameworks, "not true" may not be "false" and "not false" may not be "true".

The simplest logic formulas are so-called atomic formulas, which represent either the existence of some property of the elements, or the existence of a relationship between the elements. This group also includes the formula for knowledge – $A \int B$.

Let us recall that X is information if it is knowledge or data, or in other words:

- there are A and B, so that $(A \int B)$ and $X=\langle A,B\rangle$, or
- there are A and B, so that $(A \int B)$ and $X=A$, or
- there are A and B, so that $(A \int B)$ and $X=B$.

Therefore, if we want to claim that X is false, we must find a formula that is false, or at least is not true. In this case, it is the formula $A \int B$.

Definition 7 (Lorents, 2007). Some information X is *false information,* if:

- there is an argument "there are A and B, so that $(A \int B)$ and $X=\langle A,B\rangle$" while $A \int B$ is *not true*, or
- there is an argument "there are A and B, so that $(A \int B)$ and $X=A$" while $A \int B$ is *not true*, or
- there is an argument "there are A and B, so that $(A \int B)$ and $X=B$" while $A \int B$ is *not true*.

Note that there is a difference between false information and non-information. At the same time, it is easy to prove that if X is false, then X is not information.

Proof. $[(\exists\alpha\beta)(P(\alpha,\beta)\&M(\alpha,\beta)\&\neg M(\alpha,\beta)) \vee (\exists\alpha\beta)(R(\alpha)\&M(\alpha,\beta)\&\neg M(\alpha,\beta)) \vee$

$\vee (\exists\alpha\beta)(Q(\beta)\&M(\alpha,\beta)\&\neg M(\alpha,\beta))] \rightarrow$

$\rightarrow \neg[(\exists\alpha\beta)(P(\alpha,\beta)\&M(\alpha,\beta)) \vee (\exists\alpha\beta)(R(\alpha)\&M(\alpha,\beta)) \vee (\exists\alpha\beta)(Q(\beta)\&M(\alpha,\beta))]$

The fact that X is not information does not always mean that X is false. False information can be very useful in information or cyber operations. For example, false information could be used for misleading the enemy about your plans, strengths and weaknesses. On the other hand, it could be used as bait – something that looks

correct and credible, but is in fact not useful for the attacker.

3.5 DESTROYING INFORMATION

Destruction of information results in a complete loss of integrity and availability. In order to define information destruction we recall that information is either knowledge or data. Data, in turn, must either have at least one notation or one denotation. Therefore, X can be information only if:

- there are A and B, so that $(A \int B)$ and $X=\langle A,B\rangle$, or
- there are A and B, so that $(A \int B)$ and X=A, or
- there are A and B, so that $(A \int B)$ and X=B.

Theorem. X is not information, if:

- there *are no* A and B, so that $(A \int B)$ and $X= \langle A,B\rangle$, *and*
- there *are no* A and B, so that $(A \int B)$ and X=A, *and*
- there *are no* A and B, so that $(A \int B)$ and X=B.

Proof. Results directly from Definition 3 and the corresponding Implication 2.

This provides us with the possible ways to destroy information (X):

1. *Destroying the objects A and B.* This will also destroy the ordered pair $X=\langle A,B\rangle$ and anything that no longer exists is also no longer information. For example, destroying a secret military installation and erasing all references (written or otherwise) to it.

2. *Destroying the notation-denotation relationship between A and B.* This way, the ordered pair $X=\langle A,B\rangle$ may still exist, but it is no longer knowledge, because it lacks the notation-denotation relationship. For example, creating a false identity for Joe Smith. Both the original name (notation) and the original person (denotation) still exist, but the person is no longer associated with the old identity.

3. *Destroying all objects, which are notations or denotations for X.* If X has no notations or denotations, then X is a nameless, pointless thing. For example, if X is knowledge about the password to a particular user account, then erasing that account effectively destroys the value of the password (as knowledge).

4. IT AND CYBER WEAPONS

Let us explore the concept of a weapon in the world of systems. First, it is important to differentiate between *things that may be used as a weapon* and *things that were designed as a weapon*.

Definition 8. A *weapon* is a system that is designed to damage the structure or operations of some other system(s). (Lorents, 1998)

Weapons can include systems that deal kinetic, thermal and electromagnetic damage, as well as chemical compounds and biological organisms, etc. Therefore, it should not be surprising that there can also be weapons that work in the information systems.

Definition 9. An *information technology weapon*, or shorter – *IT weapon*, is an information technology-based system (consisting of hardware, software and communication medium) that is designed to damage the structure or operations of some other system(s).

For example, an IT system that is designed to analyze the sensor feeds to provide an accurate location for an enemy tank (to be destroyed by missiles) can be called an IT weapon.

Definition 10. A *cyber weapon* is an information technology-based system that is designed to damage the structure or operations of some other information technology-based system(s).

For example, a software tool that allows generating unnecessary network traffic for a web server is a cyber weapon. Similarly, a software tool that is designed to copy confidential user information (for example, login credentials) without the knowledge and consent of the user is a cyber weapon, because it breaches the (presumed) confidentiality requirement of the system's operations.

Note that every cyber weapon is also an IT weapon, but the opposite is not true. The targets of cyber weapons are located in cyberspace, which reinforces the connection with the "cyber" prefix.

5. CYBER INCIDENTS, ATTACKS, CONFLICTS AND WAR

The core concept in information technology is naturally information. It is both the key protected asset and the key target in the contested ground of cyberspace. There-

fore, we provide the important definitions for offensive cyber operations.

Definition 11. Cyber incidents are events that cause or may cause unacceptable deviation(s) in the structure or operation of an information system (or its components, including information, hardware, software, etc.).

Cyber incidents can be accidental (for example, a power outage causes the system to stop working) or intentional. Furthermore, they can be the effects from events in cyberspace or physical effects.

Definition 12. Cyber attack is the intentional use of a cyber weapon or a system that can be used as a cyber weapon against an information system in order to create a cyber incident.

For example, launching a distributed denial of service attack with a botnet, or infecting target systems with malware that disables them.

Definition 13. Cyber espionage is the use of cyber attacks to cause a loss of confidentiality of the target system.

For example, exploiting a vulnerability in the target system's configuration to gain access to confidential files.

Definition 14. Cyber conflict is the use of cyber attacks (which must include attacks against integrity or availability of the target systems) to achieve political aims.

The requirement for integrity or availability attacks comes from the fact that cyber conflicts are different from cyber espionage. While espionage can also be part of a cyber conflict, it can exist separately (and often does). Conflict, however, implies activities that either damage the target (integrity) or make it unusable (availability). The political aim in this definition is an umbrella term that is meant to include nationalism, religion, philosophy, etc., as the underlying reason for the conflict. An example of cyber conflict is the cyber attack campaign against Estonia in 2007.

Definition 15. Cyberwar is a cyber conflict between state actors.

While cyber conflicts can take place between state actors, non-state groups and individuals, a war is limited to state actors. For example, military specialists using cyber attacks to disable enemy command and control systems before a decisive ground and air attack.

Note that in this definition we are not necessarily concerned with the definition of warfare provided by contemporary international law, which may or may not be applicable to conflicts in cyberspace, depending on the interpretation (Schmitt, 1999, 2002). Instead, we provide the definition as part of a conceptual framework.

6. SUMMARY

Cyber attacks can be used in new forms of expression and conflict. In order to describe and study these events, we need a solid framework of definitions. In this paper we have covered the basic concepts of knowledge, data and information. From this, we provided definitions for information systems and intelligent systems, as well as information technology weapons and cyber weapons. With this foundation in place, we explored the three basic concepts of securing information systems – confidentiality, integrity and availability, and included two special cases of breaking these concepts: destruction and falsification of information. Lastly, we provided definitions for the concepts of cyber incident, cyber attack, cyber espionage, cyber conflict and cyberwar.

REFERENCES

- Birkhoff, G., von Neumann, J., 1936. The logic of quantum mechanics. *Ann. Math.* 37, 823–842.
- Cohn P. M., 1965. *Universal Algebra*. Evanston: Harper&Row.
- Grätzer, G., 2008. *Universal Algebra*. Second Edition. Springer.
- Hartley, R. V. L., 1928. Transmission of Information. *BSTJ* 7, 3, pp 535-563.
- Lorents, P., 1998. *Süsteemse käsitluse alused. Riigikaitse ja julgeoleku põhiküsimused.* (Foundations of the Systemic Approach. Main Problems of National Defence and Security.) Tallinn: Eesti Riigikaitse Akadeemia kirjastus.
- Lorents, P., 2001. Formalization of data and knowledge based on the fundamental notation-denotation relation. *Proceedings of the International Conference on Artificial Intelligence*. IC – AI' 2001. Vol III, pp 1297-1301.
- Lorents, P., 2001b. *Informaatika teoreetilised alused. Struktuurne aspekt.* (Theoretical Foundation of Informatics. Structural Aspect.). Tallinn: EBS Print.
- Lorents, P., & Lorents, D., 2003. Intelligence and the notation-denotation relation. *Proceedings of the International Conference on Artificial Intelligence*. IC – AI' 2003. Vol II, pp 703-707.
- Lorents, P., 2005. The role of equality in knowledge acquisition. *Proceedings of the International Conference on Artificial Intelligence*. IC – AI' 2005. Vol II, pp 555-561.
- Lorents, P., 2006. *Süsteemide maailm* (The World of Systems). Tartu: Tartu Ülikooli Kirjastus.
- Lorents, P., 2007. Denotations, Knowledge and Lies. *Proceedings of the International Conference on Artificial Intelligence*. IC-AI' 2007. Las Vegas, US, June 14-17, Vol II, pp 324-329. CSREA Press.
- Lorents, P., 2008. Knowledge and Taxonomy of Intellect. *Proceedings of the International Conference on Artificial Intelligence*. IC-AI' 2007. Las Vegas, US, July 25-28, Vol II, pp 484-489. CSREA Press.
- Lorents, P., Ottis, R., Rikk, R., 2009. Cyber Society and Cooperative Cyber Defence. *Internationalization, Design and Global Development*. Lecture Notes in Computer Science, Vol 5623, pp 180-186.
- Maltsev, A. I. (Мальцев А. И.), 1970. *Алгебраические системы* (Algebraic systems). Moscow: Наука.
- Ottis, R., & Lorents, P., 2010. Cyberspace: Definition and Implications. *Proceedings of the 5th International Conference on Information Warfare and Security*. ICIW 2010. Dayton, US, 8-9 April. [accepted for publication]
- Schmitt, M., 1999. Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, Vol 37, pp 885-937.
- Schmitt, M., 2002. Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, Vol 84, No 846, pp 365-399.
- Shannon, C. E., 1949. Communication in the presence of noise. *PIRE*, 37, 1, pp 10-21.
- Tuller, W. G., 1949. Theoretical limitations on the rate of transmissioon of information. *PIRE*, 37, 5, pp 468-478.
- Tyugu, E., 1988. *Knowledge-Based Programming*. London: Addison-Wesley.
- Tyugu, E., 2007. *Algorithms and Architectures of Artificial Intelligence*. Amsterdam: IOS Press.
- Wiener, N., 1948 *Cybernetics: Or Control and Communication in the Animal and the Machine*. New York: John Wiley.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

OPTIMIZING IT SECURITY COSTS BY EVOLUTIONARY ALGORITHMS

Toomas Kirt[a,1], Jüri Kivimaa[b,2]

[a] *University of Tartu, Estonia,* [b] *CCD COE, Tallinn, Estonia*

Abstract: One of the most critical issues in IT security is to establish a cost-effective framework for cyber protection against possible threats. The overall security framework is divided into security activity areas, which can have a number of protection levels. Each level of one security activity area provides certain confidence and also requires some expenditure. As the budget level is predefined a critical question remains how to find out an adequate security profile for a certain cost level. As the behavior of cyber attackers and cyber security threats are continuously changing, there should not be just one model to construct an effective security mechanism but rather a variety of changing alternatives. Several methods have been proposed for cost optimization but they are limited by providing only one alternative. In this paper we propose an evolutionary approach as an alternative for optimizing IT security costs and for finding variants of security profiles for every cost level. Higher variability of security profiles will make the security organization more resistant to changing cyber attacks.

Keywords: graded security model, information security metrics, information security requirements, evolutionary computing, genetic algorithms

1 University of Tartu, Institute of Public Law, Teatri väljak 3, Tallinn, 10143, ESTONIA, Email: Toomas.Kirt@ut.ee.

2 Cooperative Cyber Defence Centre of Excellence, Filtri Street 12, Tallinn, 10132, ESTONIA, Email: Jyri.Kivimaa@ccdcoe.org

INTRODUCTION

We have the challenge of ensuring information security under conditions of uncertainty: how can organizations determine appropriate measures to enhance cyber security and allocate resources most efficiently? For finding out an optimal amount of resources a security costs function is proposed, where the total cost of security for a system is based on the cost of system security investments plus the cost of damage and cost of recovery from any security incidents (Olovsson, 1992). Despite the fact that the cost function also includes indirect costs in this study we take into account only the direct costs of security investments. Usually, available resources are limited and therefore it is needed to optimize applied security measures to achieve the highest attainable confidence level. The security framework is divided into several security activity areas that can have a number of levels providing certain confidence. As the number of security activity areas increases the number of different combinations of security measures or profiles grows exponentially. For finding an optimal security profile several optimization methods are used, such as a brute force optimizer and a discrete dynamic programming method (Kivimaa, 2009; Ojamaa, Tyugu, & Kivimaa, 2008).

It is argued that the dynamic programming may have some problems related to independence of security activity areas and additivity and therefore the solutions may not to be optimal (Kivimaa, 2009). This additivity restriction also limits the search space and it is difficult to find out alternative security profiles that provide the same level of confidence. Therefore our aim is to apply an additional method to find out whether the solutions are adequate and also identify alternative security profiles for a certain cost level. We decided to use an evolutionary algorithm as a universal method for complex optimization in many fields. Genetic algorithms are also actively used in IT security and intrusion detection systems (e.g. Li, 2004; Sinclair, Pierce, & Matzner, 1999).

Evolutionary algorithms are based on a Darwinian natural selection process and form a class of population-based stochastic search algorithms (Dracopoulos, 2008; Eiben & Smith, 2003; Holland, 1975). In the evolutionary process for all the individuals representing candidate solutions some perturbations (e.g. crossover, mutations) are applied to generate variation and thereafter a selection procedure, based on the value of a fitness function, is enforced. The selection mechanism prefers individuals that are the best candidates for the solution of the optimization problem. To maintain the variation in population in our experiments the population was divided into subgroups and the selection process was performed within a group. This measure helped to avoid the optimization process to fall into a local optimum and provided better results. To solve the optimization task we have established an evolutionary framework and applied it to the IT security cost/confidence data consisting of 9 se-

curity areas (CyberProtect, see Table 1). In the following optimization tasks we had two goals: to minimize the costs and to maximize the integral security confidence.

This paper is divided into four main parts. In the first part the security model and the data is described that we use in our optimization tasks. Next we introduce the basis of evolutionary algorithm. Thereafter the results of optimization are given. Finally the results are discussed and conclusions are made.

1. SECURITY MODEL

The main challenge in IT security is to ensure required information security under conditions of uncertainty. To achieve the goal an organization has to define adequate security levels and to determine appropriate measures for increasing cyber security and allocating resources most efficiently. Usually certain risk assessment methods are used for performing detailed risk analysis. For small and medium size enterprises the detailed risk analysis is relatively expensive and also the available resources for IT security are limited. Therefore a simpler version of the security model is needed which provides possibility to achieve maximum possible confidence with limited resources.

Table 1. IT security costs/confidence data. 9 security measures

Security measure \ level		Level 0	Level 1	Level 2	Level 3
1. User Training	Cost	0	4	8	12
	Confidence	0	30	50	65
2. Redundant Systems	Cost	0	8	10	12
	Confidence	0	40	70	95
3. Access Control	Cost	0	1	2	4
	Confidence	0	40	70	95
4. Antivirus	Cost	0	2	4	7
	Confidence	0	60	80	95
5. Backup	Cost	0	1	2	4
	Confidence	0	40	70	95
6. Disconnection	Cost	0	2	4	7
	Confidence	0	40	60	75
7. Encryption	Cost	0	2	4	7
	Confidence	0	60	80	95
8. Firewall	Cost	0	2	4	7
	Confidence	0	30	50	65
9. Intrusion Detection	Cost	0	1	2	4
	Confidence	0	25	45	60

In this research we rely on the graded security model, which is an improved and combined version of two security methodologies: the US DoE graded security methodology (best practice security methodology to specify needed security measures for needed security levels; DOE, 1999) and Estonian governmental data classification (metrics to specify needed security level; ISKE, 2009). "The system includes knowledge modules (rule sets) in the form of decision tables for handling expert knowledge of costs and confidence, as well as for selecting security measures for each security group depending on the required security level." [Kivimaa, et. al., 2009] Basic ideas of graded security are presented as a decision table – information security activities areas/their realization levels and information security requirements/their levels in a dependency matrix. As an example a very simple (9 security subareas) decision table/dependency matrix is given in the Appendix.

The example used in the experiments of this paper is an educational security framework CyberProtect version 1.1 (CyberProtect, Table 1). It determines how hardware/software/firmware can be secured based on nine security activity/measure groups and their high/middle/low level realization of costs and confidence. The cost in this example covers only the costs of security investments and is given in conventional units. The confidence level is in the scale of 0···100 and the value is provided as an expert opinion. Each security measure can have a certain level that determines required resources to achieve confidence. The baseline security methodologies define conventional goals of security as confidentiality (C), integrity (I), availability (A), and mission criticality (M). For each goal a finite number of security levels have been determined. For example, four levels 0, 1, 2, 3 for representing required security and protection can be used, where the lowest level 0 denotes unnecessary of special protective measures. [Kivimaa, et. al., 2009]

We can formulate an optimization problem as follows: find the abstract security profile with the best (highest) value of confidence for given amount of resources. As we have a limited amount of available resources r our goal is to achieve a maximum security level

$$S_{\max} = \sum_{i=1}^{n} a_i q_{\max i}$$

where $q_{\max i}$ is maximum security confidence of the i-th group of security activity areas and a_i is the weight of the i-th group

$$\sum_{i=1}^{n} a_i = 1$$

We have an optimization problem with two goals: to minimize resources on the interval $[r_{min}; r_{max}]$ and to maximize security, guaranteeing at least the levels prescribed by a given security class. We are going to solve this problem by finding a function that gives an abstract security profile that has maximum value of a security confidence function given by the weighted mean security for any given value of resources on the interval $[r_{min}; r_{max}]$. The task of the optimization application is to find the best combination of security measure levels that provides the maximum confidence at a cost level.

In previous experiments mainly two optimization algorithms were used to solve our task – one of them was a brute force optimizer and the other one was based on a Pareto optimality (Pareto frontier or Pareto set) and discrete dynamic programming method (Ojamaa, et al, 2009). This problem can be solved by means of building a Pareto optimality trade-off curve that explicitly shows the relation between used resources and security confidence. Then, knowing the available resources, one can find the best possible security level that can be achieved with the resources and specify the security measures to be taken.

For n security measures groups and k levels for information security requirements/goals we have totally k^n abstract security profiles to be considered. The number of security measures groups may be in practice up to 30 or even more and in Estonian data classification a 4-level version for security goals is used. This gives a number of abstract security profiles: 4^{30}.

With the brute force method we must do rk^n computations and with the dynamic programming method r^2kn (r is number of possible values of resources, k is the number of security levels, n is number of security measures groups). For example, if we have a 100 budget points curve for 25 security subareas then it takes ~10 seconds to calculate it with the Pareto optimality & dynamic programming and by the Brute Force method it would take ~10 years to calculate (Kivimaa, 2009).

To use Pareto optimality and dynamic programming in optimization security activities areas/security measures groups must be not dependent from each other's and their security measures to realize their levels must be additive. Independency in IT security activities is quite problematic for some security areas, but in first approximation it is acceptable if we use certain specific logic of description (for example, the IT security experts/specialists training costs are included into the costs of concrete security activities areas/areas levels and some other analogical principles might be followed).

The second weakness of dynamic programming is that it has some difficulties in finding alternative security profiles for a certain optimal cost/confidence level. To get over those weaknesses and to measure adequacy of the dynamic programming

we decided to use an evolutionary algorithm as an alternative method. We expect that the evolutionary approach is not stuck to such limitations and can provide results with a quite reasonable time.

2. EVOLUTIONARY ALGORITHMS

An evolutionary algorithm is a population-based stochastic search algorithm. The basic principle is to iteratively generate random variation within individuals of population, that represents the candidate solution to the problem, and to select the fittest candidates that provide the best solution to the task in hand. The view that random variation provides the mechanism for discovering new solutions (Michalewicz & Fogel, 2004) was inspired by the process of natural evolution.

The idea of using Darwinian principles of evolution to solve some combinatorial optimization problems arose with the invention of computers. Afterwards several approaches were developed like evolutionary programming (Fogel, Owens, & Walsh, 1966) and genetic algorithms (Holland, 1975) in the early stage of the study of evolutionary algorithms. Now there are a wide variety of approaches that can be described as belonging to the field of evolutionary computing. The algorithms used in the field are termed as evolutionary algorithms (Dracopoulos, 2008). The most important characteristics of evolutionary algorithms are as follows:

- *Representation.* Each candidate solution to the problem in hand is represented as an individual. The characteristics of the individual are encoded by genes. The set of individuals form a population.
- *Fitness.* The quality of a candidate solution is measured by a fitness function. The fitness function is used to measure how good an individual is. Fitter solutions have a higher probability to survive and to contribute their characteristics to offspring.
- *Variation.* Variation operators (e.g. crossover, mutations) are applied to the individuals that modify the population of solutions dynamically.
- *Selection.* The average fitness is improved over time as a selection mechanism is applied and the fittest individuals are selected for the next generation (survival of the fittest).

The basis of an evolutionary algorithm is simple. First, a population of initial candidate solutions has to be generated randomly. Thereafter iteratively a number of variation generation operators are applied and new generations are selected based on the fitness values of individuals.

2.1 ALGORITHM

There are several modifications proposed to the basic algorithm and we have adapted some aspects of cooperative co-evolutionary algorithms (see Machado, Tavares, Pereira, & Costa, 2002; Potter & De Jong, 2000). In this approach the problem is decomposed into subcomponents that represent potential components to the global problem (see more details in Selection). As the problem in hand was not very complex we decided to decompose a population P into S subpopulations Ps instead of decomposing a problem. The aim was to maintain variety within the population as a whole.

The algorithm can be defined then as follows:

- for each subpopulation S do:
  - Initialize population Ps(0)
  - Evaluate all individuals from Ps(0)
- While termination condition not met repeat:
  - For each subpopulation S do:
    - Apply crossover and mutation operators to individuals of Ps(t) and obtaining a set of offspring Os(t)
    - Evaluate individuals from Os(t)
    - Combine Ps(t) and Os(t) obtaining Ps(t+1)

During the evaluation the fitness value (average confidence level) of an individual is found. The fittest from the ordered set of parents and offspring are selected for the next generation.

2.2 REPRESENTATION

How to choose a suitable genetic representation of an individual is a key issue in evolutionary computing. Each individual has two representations: phenotype (outside) and genotype (inside). Object forming possible solutions within the original problem context are referred as phenotypes, while their encoding, that is, the individuals within the evolutionary algorithm, are called genotypes (Eiben & Smith 2003). Phenotypic characteristics of the candidate solution are encoded by individual's genotype. The genes are the functional units to carry inherited information and they can be arranged in chromosomes. In evolutionary algorithm a chromosome can be a string of symbols or a vector of numerical variables (Gen & Lin, 2008). The complete inherited information is called a genome.

Genotype contains inherited information to build an individual in phenotype space. In the natural systems the mapping from genotype to phenotype is not direct. In the context of evolutionary algorithms three classes of possible mappings are defined: direct, developmental and implicit (Floreano, Dürr, & Mattiussi, 2008). In a direct representation, there is a one-to-one mapping between the parameter values of the task in hand and the genes that compose the genetic string. In developmental representations which are used mostly in case of large problems the specification of a developmental process is genetically encoded which in turn constructs the desired phenotype. In case of implicit encoding like in biological gene networks, the interaction between the genes is not explicitly encoded in the genome, but follows implicitly from the physical and chemical environment in which the genome is immersed.

In this paper direct mapping is used and each candidate solution is represented as a chromosome consisting of the same amount of genes as the number of security activity areas. Each gene denotes a security level of one security activity area. For example, if there are 3 security levels plus one for the lowest level 0 denoting absence of special protective measures four possible values for one gene (0, 1, 2, 3) can be defined. If there are 9 security activity areas then a chromosome can be G = {1 0 3 2 3 1 2 1 3}.

2.3 FITNESS

The goal of the evolutionary search is defined as a user-specified measure of the quality or the fitness of the individuals. The algorithm is expected to find in the search space an individual with maximum quality or fitness. In our experiments the fitness is measured as a weighted average of confidence levels of security activity areas.

2.4 VARIATION

The initial population is usually generated randomly and therefore it is highly variable. The movement in the search space is based on random changes in chromosomes generated by reproduction and applying several variation operators. The reproduction is carried out with some stochastic mutation and recombination of the parents in order to explore new regions the search space and combine the information carried by each parent (Gen & Lin, 2008).

The main operator to generate variation in population is the crossover. There are introduced several approaches to select parents and to recombine their genetic information. Recombination, the process whereby a new individual is created from the information contained within two parents, is considered to be one of the most

important features in evolutionary algorithms. In the experiments we use the crossover operator called n-point crossover, where the value of n is 2. The basic steps of applying a crossover operator are as follows: first, to select two parents based on some restrictions (if there are any) and next, select segments of genes from both parents to form the genes of an offspring. The second parent is selected randomly from the whole population. An example is illustrated in Figure 1. A segment {4, 3} is taken from one parent and is transferred to the other parent's genetic code.

Figure 1. n-point crossover. n = 2.

Several variation operators are used to make variation in population and to move in the search space.

Random mutation is the change of the value of one gene. For example, the value of the first gene {1} is replaced by the new value {3}.

Figure 2. Random mutation of a single gene

Swap operator: selects two genes and swaps them. For example, genes {5} and {3} are selected and swapped.

Figure 3. Swap mutation

Inversion operator: selects a segment of genetic code and reverses order of the genes belonging to it. For example, genes {1 5} are reversed {5 1}.

Figure 4. Inversion mutation

Insertion operator: selects a gene and inserts it in another place. For example, gene {1} is moved to the end of the genetic code.

Figure 5. Insertion mutation

Displacement operator: selects a segment of genetic code and inserts it in another place. For example, genes {1 5} are moved to the end of the genetic code.

Figure 6. Displacement mutation

When mutation operators are applied, the genes are validated whether they are in accordance to the restrictions of the task in hand. When the code does not meet the restrictions it is not used in the further processing.

2.5 SELECTION

The selection is a process to select survivals for the next generation. During each generation, the chromosomes are evaluated, using some measures of fitness. A new generation is formed by selecting some parents and offspring, according to their fitness values, and rejecting others to keep the population size constant.

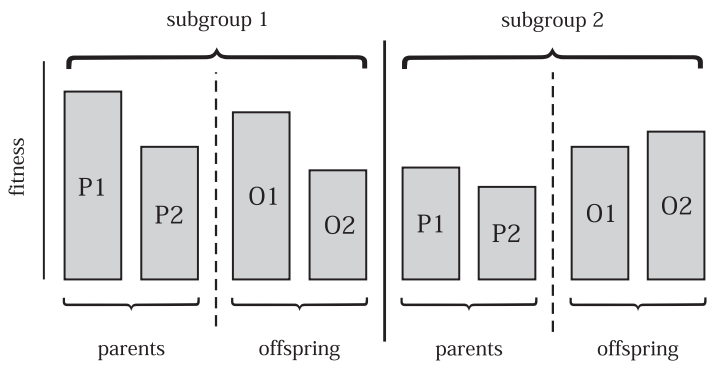

Figure 7. An example of a tournament selection of 2 sub-population consisting of 2 individuals. 4 candidates (2 parents P and 2 offspring O) are competing for selection for next generation within a sub-population

a) After reproduction and mutation a new sets of individuals (offspring) are formed in each subpopulation

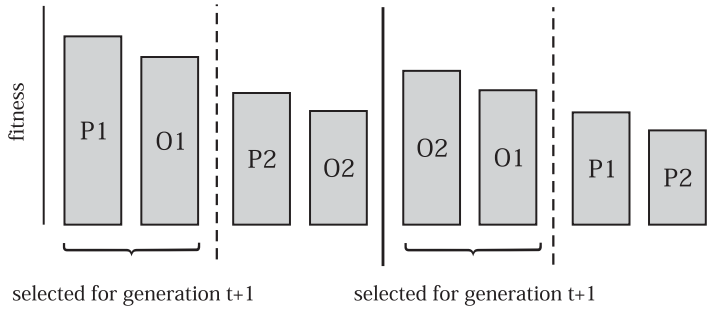

Figure 8. Selection and regrouping of the initial population.

b) For selection the parents and offspring within a sub-group are ordered based on the fitness value and the fittest are selected for the next generation

In this study the selection method is based on the tournament selection strategy, which is deterministic. The tournament selection is effective, because it does not require any global knowledge of the population and it also avoids falling into a local optimum by maintaining variety in the population. This strategy also enhances the search space and allows exploring it in parallel. To perform tournament selection we have to define the tournament size k. The members of a tournament are usually selected randomly, but we use a deterministic strategy where the competing sub-populations are predefined. For example, the tournament or subpopulation size is defined as 2. After reproduction and mutation phase (Figure 7) 4 candidates (2 parents and 2 offspring) compete for being selected for the next generation (Figure 8). The selection is performed locally and therefore the winning members of one tournament may have a weaker fit value than the least-fit members of the other tournament. Further mutations in such a weak subpopulation may reveal some properties of an individual that are needed to reach the global optimum and are not represented in other subgroups.

3. EXPERIMENTS

For experiments we had the IT security cost/confidence data consisting of 9 security activity areas (CyberProtect; see Table 1). The aim of the optimization was to find the highest average confidence level for a given amount of resources. The optimization task is formed as a question (Kivimaa, 2009): “For every possible budget level, what is the maximum confidence one can expect?” In the optimization tasks the amount of resources (budget) was predefined form 1 to max+1. The max value equals the costs of the security measures of the highest level.

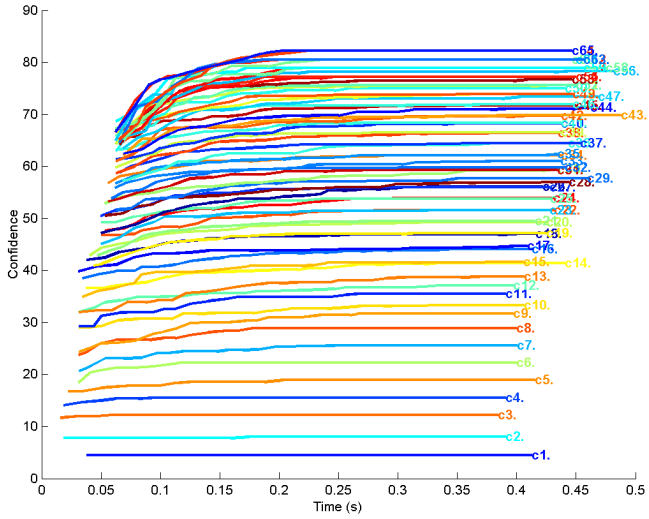

Figure 9. **Mean computational time to find optimal confidence value for 9 security areas (mean value of 5 experiments)**

The first task was to measure the mean computational time to solve the optimization problem. The second task was to find the cost/confidence optimality curve. The third task was to find out the cost/confidence optimality curve when the optimality was restricted by a security class. The fourth task was to identify adequate and equivalent security profiles for every cost level.

For the results presented in this section we used the following experimental settings: crossover rate 0.49, mutation rate 0.2, swap rate 0.1, inversion rate 0.1, insertion rate 0.1, and displacement rate 0.1. The number of generations was set as 30 and population size 80, and the tournament or subpopulation size was 5. The cost of the highest security level (C3I3A3M3) was 64 units and the optimization was performed for the cost levels from 1 to 65 units. With each cost level 5 experiments were performed. The rates for crossover and mutation operators were selected as the best practice of solving other optimization problems. Despite the optimization tasks are similar the rates might not be the best for solving the security optimization task. Additional computation time is required if either the variation rate is very low or high, as unnecessary calculations are needed to be performed.

As a result the average time for optimization was between 0.4 and 0.45 seconds (Figure 9). The task two was to find the cost/confidence optimality curve (yellow dots in Figure 10). For interpretation a color coding of dots in the curve is used as follows: red dots – all security activities area's security levels are ≤ and at least one is < than required; green dots – all security goals/their required levels are exactly achieved;

yellow dots – at least one security level is less and at least one security level is more than required; blue dots – all security levels are ≥ and at least one security level is > than required. The curve represents the optimal value of weighted mean security confidence depending on the resources that are used.

Table 2. The experimental dependency matr ix of 9 security measures

Security measure	C0	C1	C2	C3	I0	I1	I2	I3	A0	A1	A2	A3	M0	M1	M2	M3
1. User Training	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
2. Redundant Systems	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
3. Access Control	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
4. Antivirus	1	1	2	3	1	1	2	3	1	1	2	3	1	1	2	3
5. Backup	0	1	2	3	0	1	2	3	0	1	2	3	0	1	3	3
6. Disconnection	1	1	2	3	1	1	2	3	1	1	2	3	1	2	3	3
7. Encryption	0	0	1	3	0	1	2	3	0	0	0	0	0	0	2	3
8. Firewall	0	1	2	3	0	1	2	3	0	1	2	3	0	2	3	3
9. Intrusion Detection	0	1	2	3	0	1	2	3	0	1	2	3	0	2	2	3

Next experiments were performed when the limitation of security class was applied. In this study an experimental dependency matrix of connections between security measures and conventional goals of security was used (Table 2). For example, as the security class is defined C1I1A1M1 then the highest level of a security measure is selected and the security configuration is (1, 1, 1, 1, 1, 2, 1, 2, 2). The comparison of confidence values between the security classes C3I3A3M3 and C1I1A1M1 is given in Figure 10. As there are more available resources than are needed to satisfy the restrictions caused by a security class the security measures cannot be weaker than determined by the security class.

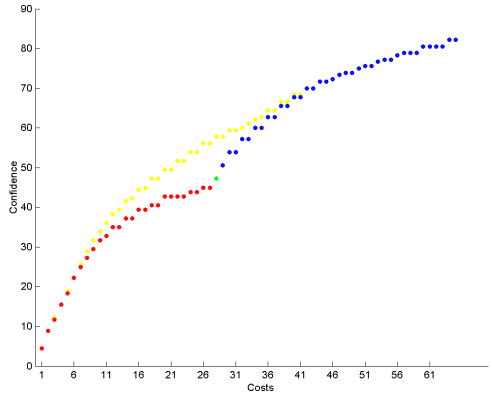

Figure 10. Costs/confidence optimality curve using security-class limitation. Security class C3I3A3M3 versus C1I1A1M1. Optimal security configuration (1, 1, 1, 1, 1, 2, 1, 2, 2)

The final task was to obtain different security profiles. To find out different security profiles we ran experiments 35 times for every cost level. An extract of the results is given in Table 3. For example, when 34 unit of money was available (budget restriction) then 5 equivalent security profiles were found.

Table 3. Equivalent security profiles for every cost/confidence level in case of 9 security measures. An excerpt

				Security measure								
No.	Money	Costs	Confidence	1	2	3	4	5	6	7	8	9
…												
88	34	34	62,22	1	4	4	2	4	2	3	3	3
89	34	34	62,22	1	4	4	3	4	2	2	3	3
90	34	34	62,22	1	4	4	3	4	3	2	2	3
91	34	34	62,22	1	4	4	2	4	3	3	2	3
92	34	34	62,22	1	4	4	2	4	3	2	3	3
93	35	35	62,78	2	1	4	3	4	4	3	3	4
94	35	35	62,78	2	1	4	3	4	3	4	3	4
95	35	35	62,78	2	1	4	3	4	3	3	4	4
96	35	35	62,78	2	1	4	4	4	3	3	3	4
97	36	36	64,44	1	4	4	3	4	3	3	2	3
98	36	36	64,44	1	4	4	2	4	3	3	3	3
99	36	36	64,44	1	4	4	3	4	2	3	3	3
100	36	36	64,44	1	4	4	3	4	3	2	3	3
…												

4. CONCLUSIONS

The aim of the study was to evaluate whether the evolutionary approach is applicable to the security of the cost/confidence optimization task and whether it allows us to generate equivalent security profiles for every cost level. As a result we could conclude that the evolutionary approach is viable for such tasks. The results indicated that the evolutionary algorithm was fast enough to provide results and turned out to be more flexible than the discrete dynamic programming method. The evolutionary approach provided results within a reasonable time limit and the cost/confidence optimization of 9 security activity areas took 0.4-0.45 seconds (Figure 7). The main advantage of the evolutionary algorithm was that it provided several adequate and equivalent security profiles for every cost level with a reasonable time (see Table 3). As it is noted, there should not be just one model to construct an effective security mechanism but several simple security mechanisms that are attuned to the needs of differing applications and organizations (Wulf & Jones, 2009). Thereby the evolutionary approach might help us to provide a better confidence level.

REFERENCES

- CyberProtect, version 1.1. U. S. Department of Defense, Defense Information Systems Agency. Available at: from http://iase.disa.mil/eta/. [Accessed 1st February 2010]
- Department of Energy, 1999. *Classified Information Systems Security Manual.* Available at: https://www.directives.doe.gov/directives/archive-directives/471.2-DManual-2/at_download/file. [Accessed 1st February, 2010]
- Dracopoulos, D. C., 2008. Evolutionary Learning. In B. Wah (Ed.), *Wiley Encyclopedia of Computer Science and Engineering*. New York: John Wiley & Sons.
- Eiben, A. E., & Smith, J. E., 2003. *Introduction to Evolutionary Computing*. Berlin: Springer.
- Floreano, D., Dürr, P., & Mattiussi, C., 2008. Neuroevolution: From architectures to learning. *Evolutionary Intelligence,* 1(1), 47–62.
- Fogel, L. J., Owens, A. J., & Walsh, M. J., 1966. *Artificial Intelligence Through Simulated Evolution,* John Wiley & Sons: New York.
- Gen, M., & Lin, L., 2008. Genetic Algorithms. In B. Wah (Ed.), *Wiley Encyclopedia of Computer Science and Engineering*. New York: John Wiley & Sons.
- Holland, J. H., 1975. *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*. Cambridge, MA: MIT Press.
- ISKE, 2009. ISKE - three-level IT baseline protection system (Version 5.00). Retrieved February 1, 2010, Available at: http://www.ria.ee/public/ISKE/iske_rakendusjuhend_5_00.pdf. [Accessed 1st March, 2010]
- Kivimaa, J., 2009. Applying a costs optimizing model for IT security. In H. Santos (Ed.), *Proceedings of the 8th European Conference on Information Warfare and Security* (pp. 142–153). Reading, UK: Academic Publishing Limited.
- Kivimaa, J., Ojamaa, A., Tyugu, E., 2009. Graded Security Expert System, *Critical Information Infrastructure protection,* Berlin: Springer.
- Li, W., 2004. Using Genetic Algorithm for network intrusion detection. In *Proceedings of United States Department of Energy Cyber Security Group 2004* Training Conference (pp. 1-8). Kansas City, Kansas.
- Machado, P., Tavares, J., Pereira, F. B., & Costa, E., 2002. Vehicle Routing Problem: Doing it the Evolutionary Way, In *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2002)* (p. 690). New York, USA.
- Michalewicz, Z., & Fogel, D. B., 2004. *How To Solve It: Modern Heuristics*. Berlin: Springer.
- Ojamaa, A., Tyugu, E., & Kivimaa, J., 2008. Pareto-optimal situation analysis for selection of security measures. In *Military Communications Conference: Unclassified Proceedings* (pp. 3224–3230). Piscataway, NJ: IEEE.
- Olovsson, T., 1992. A Structured Approach to Computer Security. In: *Technical Report No. 122*. Göteborg, Sweden: Chalmers University of Technology.
- Potter, M. A., & De Jong, K., 2000. *Cooperative Coevolution: An Architecture for Evolving Coadapted Subcomponents.* Evolutionary Computation, 8(1), 1–29.
- Sinclair, C., Pierce, L., & Matzner, S., 1999. An application of machine learning to network intrusion detection. In *Proceedings of the 15th Annual Computer Security Applications Conference* (pp. 371-377). Phoenix, AZ.
- Wulf, W. A., & Jones, A. K., 2009. Reflections on Cybersecurity. *Science,* 326, 943–944.

APPENDIX

Table 4. The dependency matrix of 9 security measures

NO	Information Security Goals / Information Security activities areas	Confidentiality Requirements				Integrity Requirements				Availability Requirements				Mission Criticality			
		C0	C1	C2	C3	I0	I1	I2	I3	A0	A1	A2	A3	R0	R1	R2	R3
		Public Data	Data for Internal Use	Confidential Data	Highly Confidential Data	Protection/Detection of Changes is Not Important	Protection/Detection of Unauthorized Changes	Inputter/Changer must be detectable	Inputter/Changer Must be Provable (in court)	Delay of Data Will Not Cause Problems	Availability 90% - allowed ~ one day delay in week	Availability 99% - allowed ~ one hour delay in week	Availability 99,9% - allowed one ~10 minuts delay in week	Data Delay Will Not Cause Significant Consequences	Data Delay Causes Damages in Hundreds of Thousands	Data Delay Causes Damages in Millions of Kroons	Data Delay Causes Hundreds of Millions of Damages
1.	**Access Control**	AC-0	AC-1	AC-2	AC-3	AC-0	AC-1	AC-2	AC-3								AC-4
2.	**User Training**		UT-1	UT-2	UT-3												
3.	**Disconnection** (Data Communications)		DC-1	DC-2	DC-3						DC-1	DC-2	DC-3				DC-4
4.	**Encryption**		CR-1	CR-2	CR-3		CR-1	CR-2	CR-3								
5.	**Intrusion Detection** (Monitoring)	ID-0	ID-1	ID-2	ID-3												
6.	**FireWall** (Perimeter Protection)	FW-0	FW-1	FW-2	FW-3	FW-0	FW-1	FW-2	FW-3								
7.	**Antivirus**		AV-1	AV-2	AV-3		AV-1	AV-2	AV-3								
8.	**Backup and Recovery**						BR-1	BR-2	BR-3		BR-1	BR-2	BR-3				BR-4
9.	**Redundancy** (IT Recovery)										R-1	R-2	R-3				R-4

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

PERSPECTIVES ON BUILDING A CYBER FORCE STRUCTURE

Stuart STARR[a,1], Daniel KUEHL[b,2], Terry PUDAS[c,3]

[a]*Center for Technology and National Security Policy (CTNSP), Washington, DC, USA*
[b]*iCollege of the NDU. Washington, DC, USA*
[c]*CTNSP, NDU, Washington, DC, USA*

Abstract: This paper explores the US's cyber force structure with special emphasis on the cyber workforce. To achieve that goal, this paper addresses several issues: it characterizes the nature of the cyber security problem; it draws on insights from senior decision-makers to identify cyber force structure needs; it characterizes current capabilities by summarizing the key initiatives that are being pursued by the US Services and key joint activities; and it identifies a spectrum of actions to mitigate shortfalls in the existing cyber forces structure (i.e. education; higher education and recruitment; certification, retention, professional development, and workforce management; exercises; and security clearance requirements). The paper concludes by identifying actions that NATO might pursue to improve its cyber force structure (e.g. conduct realistic, stressful exercises) and by identifying residual issues to address (e.g. career progression; value of employing "patriotic hackers").

Keywords: cyber workforce; cyber needs; cyber capabilities; residual cyber issues.

Disclaimer: The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U. S. Government. All information and sources for this paper were drawn from unclassified material.

1 Fort Lesley J. McNair, Washington, DC, USA; email: StarrS@ndu.edu.
2 Fort Lesley J. McNair, Washington, DC, USA; email: KuehlD@ndu.edu.
3 Fort Lesley J. McNair, Washington, DC, USA; email: PudasT@ndu.edu.

INTRODUCTION

The goal of this paper is to explore the US's cyber force structure with special emphasis on the cyber workforce. To achieve that goal, this paper addresses five objectives. First, it characterizes the nature of the cyber security problem. Second, it draws on insights from senior decision-makers to identify cyber force structure needs. Third, it characterizes current capabilities by summarizing the key initiatives that are being pursued by the US Services and key joint activities. Fourth, it identifies a spectrum of actions to mitigate shortfalls in the existing cyber forces structure. The paper concludes by identifying actions that NATO might pursue to improve its cyber force structure and by identifying residual issues to address.

In order to realize that goal and the subordinate objectives, this paper has employed several key sources. One of the primary sources was the conference on Cyber Force Structure that was convened at the National Defense University (NDU) in the fall of 2009. That source is complemented by White House initiatives on cyber security, testimony that was presented to the US Congress, and the results of several studies that addressed key cyber security and cyber force issues.

1. NATURE OF THE PROBLEM

Recently, ADM Dennis Blair (USN, ret.), Director of National Intelligence, presented the "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence" (Blair 2010). In that testimony, ADM Blair cited the "far-reaching impact of the cyber threat" as the primary threat facing the US. In support of that statement, ADM Blair made the following observations. He noted that "Neither the US Government nor the private sector can fully control or protect the country's information infrastructure." In particular, he noted that the "The cyber criminal sector in particular has displayed remarkable technical innovation with an agility presently exceeding the response capability of network defenders." He further observed that "Criminals are developing new, difficult-to-counter tools." and that in 2009, "we saw the development of self-modifying malware···". He concluded that "We cannot protect cyberspace without a coordinated and collaborative effort that incorporates both the US private sector and our international partners."

To support those observations, ADM Blair cited two global trends that are exacerbating the problem: network convergence and channel consolidation. Network convergence refers to the merging of distinct voice and data technologies to a point where all communications are transported over a common network structure. Channel consolidation refers to the concentration of data captured on individual users by service providers. He concluded that "··· these trends pose potential threats to the

confidentiality, integrity and availability of critical infrastructures and of secure credentialing and identification technologies."

Similarly, FBI Director Robert S. Mueller III warned that the cyber terrorism threat is "real and ⋯ rapidly expanding" (Nakashima 2010a). In his remarks he recommended strongly that companies should tell the US government when their computer systems have been attacked.

2. KEY NEEDS

As a foundation for characterizing the cyber force structure, it is important to characterize the key needs that drive the cyber force. Unfortunately, that foundation does not yet exist. However, to contribute to that discussion, the following section draws on several key products to help build that foundation.

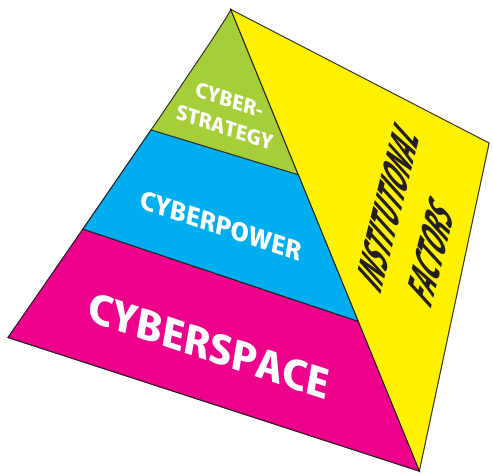

Figure 1. A Cyber Model

As an initial step, this section introduces a conceptual model that was presented in the NDU book, "Cyberpower and National Security" (Kramer, et. al., 2009). We characterize that model and identify the intellectual capital that is needed to implement that model. Second, we introduce the twelve initiatives that are subsumed within the White House's Comprehensive National Cybersecurity Initiative (CNCI) (available at www.whitehouse.gov/cyber security/comprehensive-national-cyber security-initiative). We then map those initiatives onto NDU's conceptual model to characterize the cyber force implications of those initiatives. Third, there is interest in the needs associated with a cyber attack capability. To address that issue, we

refer to the recent report that was issued by the National Research Council (NRC) on that issue (Owens, et. al., 2009). Finally, we anecdotally address the size of the cyber force by citing recent Department of Homeland Security (DHS) initiatives to hire cyber experts.

In analyzing the cyber domain, four key areas emerge (see Figure 1). These include the cyber-infrastructure ("cyberspace"), the levers of national power (i.e. diplomacy, information, military, economic, or "cyber power"), the degree to which key entities are empowered by changes in cyberspace ("cyber strategy"), and the institutional factors that affect the cyber domain (e.g. legal, governance, organization). For the purposes of this paper, this framework will be employed to decompose the problem.

Although the definitions of many of these terms are still contentious, this paper will use the following definitions for key terms. For the purposes of this theory, this white paper has adopted the formal definition of cyberspace that the Deputy Secretary of Defense formulated: "…the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries". (Deputy Secretary of Defense 2008). This definition does not explicitly deal with the information and cognitive dimensions of the problem. To deal with those aspects explicitly, we have introduced two complementary terms: cyber power and cyber strategy.

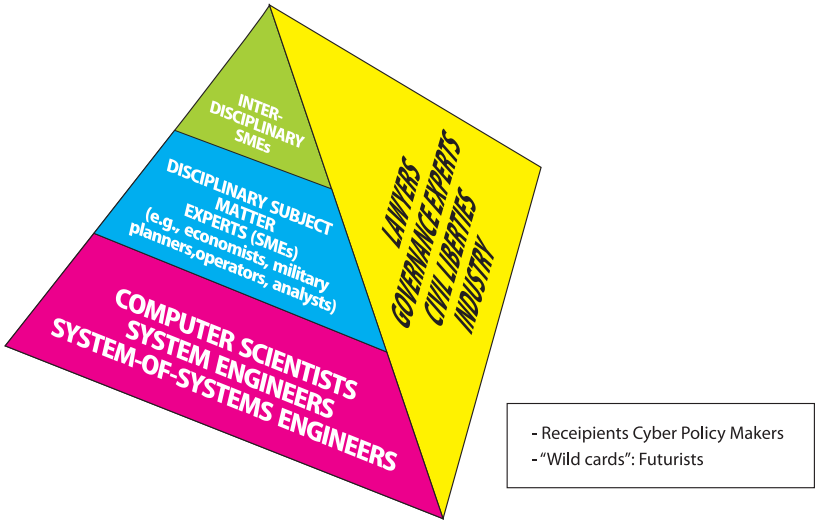

Figure 2. Required Intellectual Capital

This white paper has adopted the following definition for the term "cyber power". It is "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power." In this context, the instruments of power include the elements of the Political/Diplomatic, Informational, Military, Economic (P/DIME paradigm).

Similarly, the term "cyber strategy" is defined as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power." Thus, one of the key issues associated with cyber strategy deals with the challenge of devising "tailored deterrence" to affect the behavior of the key entities empowered by developments in cyberspace.

Finally, the other facet of the pyramid considers a spectrum of related institutional factors. These include factors such as governance, legal, organizational, and public-private relationships.

Consistent with that framework, we make the following comments about the intellectual capital that is required for each of these layers (Figure 2).

In the area of cyberspace, we are interested in the intellectual capital that is required to deal with components of cyberspace through the interdependent networks of information technology. To meet that need, there is a requirement for highly capable, *inter alia,* computer scientists, system engineers, system administrators, and system-of-system engineers. It should be emphasized that these positions cannot be filled with recent graduates or novices. There is a need for a security cleared, highly trained, and competent cadre of cyber security professionals.

In the area of cyber power, there is a need for disciplinary subject matter experts (SMEs) that are able to assess the impact of the rapid changes in cyberspace on the factors of diplomacy, information, military, and economics. For example, military planners and operational analysts have employed live, virtual, and constructive models and simulations to establish that the addition of a digital link to airborne interceptors (AIs) from an AWACS aircraft will enhance the AIs Loss Exchange Ratios by a factor of 2.5 (Gonzales, et. al., 2005). Similarly, we need SMEs to determine the functional relationships between improvements in cyberspace and the other levers of power.

In the area of cyber strategy, we need SMEs who are conversant with the empowerment of key entities (e.g. terrorists, criminals, near-peers) that emerges from improvements in cyberspace. For example, (Kramer, et. al., 2009) observes that terrorists are being empowered by cyberspace in their ability to perform a variety of key, inter-related functions (e.g. recruit, raise resources, plan and command and control

operations, conduct influence operations, and educate and train). Key features of this empowerment include low cost of entry, world-wide reach, sanctuary, and the potential to link with transnational criminals. Of particular interest is the challenge in developing a theory of cyber deterrence. To further that debate, the NRC is conducting a competition to address fifty-one questions associated with cyber deterrence (NRC 2010).

Finally, in the area of institutional factors, we need a broad set of legal, governance, and private sector experts. These include, *inter alia*, lawyers (who are conversant with cyberwar and proportional responses, differences in international versus sovereign law), governance experts (who can assess the impact of the new contract with Internet Corporation for Assigned Names and Numbers (ICANN)), and the private sector (which controls on the order of 85% of the elements of critical infrastructure).

Overall, there is a need for cyber policymakers who can synthesize these insights into coherent, meaningful policy positions. As an aside, policymakers have found it useful to have futurists who can speculate meaningfully about future directions in each level of the pyramid.

Over the last few years, the White House has aggressively supported the CNCI (Reference 5). These initiatives were begun in the administration of President George W. Bush and re-evaluated by President Barak Obama. The key features of these initiatives are summarized briefly in Table 1.

#	Initiative
1	Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections (TICs)
2	Deploy an intrusion detection system of sensors across the Federal enterprise
3	Pursue deployment of intrusion prevention systems across the Federal enterprise
4	Coordinate and redirect R&D efforts
5	Connect current cyber ops centers to enhance situational awareness
6	Develop and implement a government-wide cyber counterintelligence plan
7	Increase the security of our classified networks
8	Expand cyber education
9	Define and develop enduring “leap-ahead” technology, strategies, and programs
10	Define and develop enduring deterrence strategies and programs
11	Develop a multi-pronged approach for global supply chain risk management
12	Define the Federal role for extending cybersecurity into critical infrastructure domains

Table 1. Comprehensive National Cyber Security Initiatives

To understand the key needs associated with these initiatives, these initiatives have been mapped into the cyber “pyramid”, cited above (Table 2).

As can been seen in Table 2, we have postulated that the bulk of the CNCI initiatives are associated with cyberspace. In addition, two of the issues are associated with cyber strategy (i.e. develop a Counter Intelligence plan; develop deterrence strategies) and one is associated with institutional factors (e.g. extend cyber security into critical infrastructures domains). We have noted that initiative 8, expand cyber education, is germane to all four areas of interest. Initiative 8 identifies two key challenges. First, there are not enough cyber security experts within the Federal Government or the private sector. Second, it notes that there is not an adequately established Federal cyber security career field. To deal with those challenges, the CNCI has identified two key needs. First, there is a need to develop a technologically skilled and cyber-savvy workforce. In addition, it calls for the creation of an effective pipeline of future employees. Ultimately, there is a requirement for a national strategy on the issue.

Area	CNCI
Cyberspace*	• (#1) Manage Federal Enterprise Network as a single network enterprise • (#2) Develop intrusion detection system • (#3) Develop intrusion prevention system • (#4) Redirect Research & Development • (#5) Connect cyber centers for situational awareness • (#7) Increase security of classified networks • (#9) Develop "leap ahead" technologies • (#11) Manage global supply chain risk
Cyberpower*	
Cyberstrategy*	• (#6) Develop Counter Intelligence plan • (#10) Develop deterrence strategies
Institutional Factors*	• (#12) Extend cybersecurity into critical infrastructure domains

* (#8) Expand cyber education

Table 2. Mapping the CNCI onto the Cyber Model

In addition, the NRC (Owens, et. al., 2009) recently issued a paper that focused on the cyber force needs associated with cyber attack. Cyber attack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.

They formulated several key needs to foster a national debate on cyber attack. They concluded the following: "The US should establish a public national policy regarding

cyber attack for all sectors of government…; the US government should conduct a broad, unclassified national debate and discussion about cyber attack policy…; and the US government should work to find common ground with other nations regarding cyber attack."

Subsequently, in the section entitled "Supporting Cyber attack Capabilities and Policy", the NRC report formulated the following recommendation: "The US government should ensure that there are sufficient levels of personnel trained in all dimensions of cyber attack and the senior leaders of government have more than a nodding acquaintance with such issues."

One of the major issues associated with the cyber force need is the number of professionals that are required by it. Recently, the Department of Homeland Security (DHS) cited that it was attempting to recruit 1000 cyber specialists over the next 3 years (Nakashima&Krebs 2009)]. However, a respected subject expert on the subject, Jim Gosler, Sandia National Laboratory, postulated that nearly 20,000 to 30,000 cyber specialists would be needed to protect military, government, and private sector networks (Gosler 2010). This suggests that an enormous amount of intellectual capital will be needed to respond to the US's needs.

3. CURRENT CAPABILITIES

The Services – Army, Navy, Air Force and Marine Corps – are all taking unique and Service-specific organizational and doctrinal approaches to cyberspace. This is understandable and not necessarily bad, in that it will create more opportunities and diverse concepts for the development and even employment of cyber capabilities. This mirrors the situation in the other domains and functional environments and in that sense provides a greater menu of choices for the joint force commander to use. The drawbacks center on three potential developments. First is the possibility that there will be wasteful and unnecessary duplication of effort, which becomes even more likely with highly classified and special access programs. Second is the distinct possibility that some Service-specific capabilities will not mesh or be interoperable with other Services' programs and systems. Third, if everyone is defining cyber through the lenses of existing domains—air, land, sea, and outer space—it begs the question whether anyone is looking at cyber through a primarily cyber lens. This was the argument behind the creation of "air forces" during the period of World Wars I and II, but it also raises the question of whether military cyberspace needs its own "Billy Mitchell".

3.1 UNITED STATES AIR FORCE (USAF)

The Air Force may have been the most "visionary" Service, and its publication in 1995 of "Cornerstones of Information Warfare" signed by the then-Chief of Staff General Ron Fogelman and Secretary of the Air Force Sheila Widnall marked a key point in the Air Force's conceptual development of cyber capability (Fobelman&Widnall 1995). In 2007 the Air Force publicized its planned establishment of an Air Force Cyber Command, to stand alongside its Commands for Air Combat and Space operations. But this was widely and loudly assailed by the other Services, which saw this as a grab for "cyber turf", and as a result the Air Force modified its plan. The Air Force's organizational approach now centers on its recent creation of a numbered air force – the 24th Air Force, headquartered in San Antonio – as a component element under the Air Force Space Command (Axe 2009). There is a technical logic to this, as a tremendous amount of the Air Force's and the entire DOD's cyber connectivity resides on space-based platforms. The 24th AF's mission is to provide cyber support to the warfighter. This includes cyber situational awareness; freedom of action for friendly forces in the cyber domain; synchronization of network operations; and enabling effects in/through/from cyberspace. (Webber 2009) Functionally, these include information operations, combat communications, and network warfare. In 2007 the USAF's Scientific Advisory Board published a report on operations in a "cyber-contested" environment, which included a definition of cyberspace that included the entire electromagnetic spectrum (EMS) as the cyber domain. While this approach agrees with that used in the recent "Cyberpower and National Security" book written at the National Defense University (Franklin, et. al., 2009), the inclusion of the EMS makes it different from and more inclusive than the official DOD definition. The Air Force has a doctrine for cyberspace operations in draft, Air Force Doctrine Document 2-11, but it has remained in draft for more than two years, and prospects for a rapid issuance seem slim (Air Force Doctrine Center 2008).

3.2 UNITED STATES NAVY (USN)

The USN has also taken organizational steps to create its needed cyber capabilities. In 2006 the Chief of Naval Operations tasked his Strategic Studies Group at the Naval War College to study the implications cyberspace posed for the Navy, and they issued their report in 2007. The SSG saw cyberspace as a primary warfare area for the Navy, which would impact virtually everything the Navy does. As did the Air Force, cyberspace is driving an increasing integration of intelligence and communications, organizationally as well as operationally. In 2009 the Secretary of the Navy issued instructions designed to establish Navy-wide policy for the creation of cyber capabilities and organizations. Its intent was to insure the security and functionality of Navy supply and logistics chains, command and control systems, and

assure freedom of action in cyberspace. (Department of the Navy 2009) The Navy's most recent and important action was its recent activation of Fleet Cyber Command, with its operational element provided by the new 10th Fleet at Fort Meade, MD. The establishment in early 2010 of 10th Fleet headquarters at Fort Meade is an indication that this fleet's seas will not be liquid but rather cyber. While the Navy is still developing doctrine and concepts for the operational employment of cyberspace, this is not standing in the way of its use right now, and some have suggested that the Navy has the most effective approach. Fleet Cyber Command's most pressing needs include inspection, testing, situational awareness, operationally focused testing, use of talented people, and continuous monitoring of its networks, according to the 10th Fleet Commander, Vice-Admiral Bernard McCullough III (Montalbano 2010).

3.3 UNITED STATES ARMY (USA)

While the Army has not yet created an Army entity dedicated specifically to cyber—unlike the Navy or Air Force—the Army's concept does envision the creation of an Army Cyber Forces Command that would have the Army's Intelligence and Security Command (INSCOM) and its Network Enterprise Technology Command (NETCOM) as its two key subordinate components. Within INSCOM is the Army 1st Information Operations Command, which draws heavily on the Army's signals and intelligence communities. The Army's Combined Arms Center (CAC) at Ft Leavenworth recently released its draft Cyber-Electronics Concept of Operations (CONOPS), which is taking a very broad look at what constitutes the cyber domain, what it means to warfighting and Army operations, and what we mean by the term "cyberwarfare". The U.S. Army Training and Doctrine Command (TRADOC) approved the Army's first official cyberspace operations concept on February 5, 2010. TRADOC Pamphlet (Pam) 525-7-8, The U.S. Army Concept Capability Plan (CCP) for Cyberspace Operations (CyberOps) 2016-2028 outlines the Army's vision for integrating cyberspace operations and the use of cyberspace into the commander's overall operations. This CCP forms the baseline for the on-going Cyber/Electromagnetic Contest Capabilities-Based Assessment (CBA) that will validate required capabilities and develop solutions to get the right capabilities to commanders and soldiers. TRADOC Pam 525-7-8 takes a comprehensive look at how the Army's future force in 2016-2028 will leverage cyberspace and CyberOps. This pamphlet includes a conceptual framework for integrating CyberOps into full-spectrum operations, thereby providing the basis for follow-on doctrine development efforts. This pamphlet also establishes a common lexicon for Army CyberOps, and describes the relationship between cyberspace, the other four domains (air, land, maritime, and space), and the EMS. Lastly, it explains how converging technologies will increasingly affect Foreign Service Officer and influence capability development, thereby enabling the Army to influence the design, development, acquisition, and employment of fully integrated cyber

capabilities[2]. The CAC is exploring the implications of this new domain and how it will shape the Army's future plans, organizations, and operations (Training and Doctrine Command 2010).

3.4 UNITED STATES MARINE CORPS (USMC)

The Marines are certainly not unaware of or indifferent to the criticality of cyberspace to USMC operations. The Marine Corps focus remains support to the Marine Air-Ground Task Force (MAGTF), which is accomplished through Marine Corps Network Operations Support Center (MCNOSC). The Marines established their Marine Corps Information Operations Center in July 2009. While the Marines have had an Information Operations doctrine for several years, they do not as yet have one for cyber. The Marines are the third Service to create a major organization focused specifically on cyber, with the creation in early 2010 of Marine Forces Cyber (MARFORCYBER), with a presence at Fort Meade. MARFORCYBER will be the Marine Corps' element of the as-yet-unestablished USCYBERCOMMAND and will be the USMC's spear point for operations in cyberspace. While the MCNOSC and MCIOC are separate organizations, they will be the two key components of MARFORCYBER. Some of MARFORCYBER's key activities and responsibilities are already well established, such as network operations and SIGINT, but the real challenge will be to develop the coordination between the "2" and "6" communities: communications and intelligence. It seems apparent that most USMC activities in cyberspace will concentrate on network operations and information assurance (Marine Corps 2003, Craft 2009, Marine Corps Headquarter 2010).

3.5 OTHER ACTIVITIES

There are two major cyber changes that are likely to affect the future of the cyber force structure: the creation of the US Cyber Command and the recent issuance of the Quadrennial Defense Report (QDR).

3.5.1 US Cyber Command

In June 2009 the Secretary of Defense issued instructions for the establishment of a joint command subordinate to US Strategic Command and devoted to the cyber mission (Gates 2009). US Cyber Command is to be headed by the Director of the National Security Agency and promoted to the rank of "General". He would thus be

2 A portion of this section has been published in the *Thoughts of a Technocrat* Blog on March 12, 2010 (http://djtechnocrat.blogspot.com/2010/03/us-army-cyberspace-operations-concept.html).

"dual hated", serving simultaneously as the Director, NSA (DIRNSA) and subordinate to the Secretary of Defense, and Commander US Cyber Command and subordinate to the Commander US Strategic Command. In the new organization, both the offensive (Joint Functional Component Command for Network Warfare (JFCC-NW)) and defensive (Joint Task Force – Global Network Operations (JTF-GNO)) organizations would be folded into it. The DOD has repeatedly stressed that its role would be to protect military, not civilian, networks. This proposal has raised significant issues in the US Congress (e.g. harmonizing civil liberties and national security) and as of this writing remains under discussion and not yet confirmed by the Congress.

3.5.2 Quadrennial Defense Review (QDR)

The 2010 version of the Quadrennial Defense Review (QDR) contained a substantial discussion of the criticality of cyberspace to U.S. military plans and operations, emphasizing the need to better secure the networks and systems that make up the Global Information Grid (GIG). The 2010 QDR identified three broad goals: freedom of action in cyberspace; prevention and deterrence of conflict; and cyber support to homeland defense. The QDR poses key questions with respect to the challenge of obtaining cyber deterrence and the relationship of cyber activities to the information environment. The QDR development effort had a sub-panel devoted specifically to the cyber issue, and it drafted a "cyber strategy" that focused on the goals cited here. Since one of the key impact areas of the QDR is on resources, the DOD and Services will inevitably be affected by the QDR in the dedication of scarce resources to create capabilities in the cyber domain. The QDR outlined four steps being taken to further develop DOD's cyber capabilities. First is the need to develop a comprehensive approach to the DOD's operations in cyberspace. The next is to develop further human expertise and broaden awareness of how much the U.S. military depends on cyberspace for real military capability. Third is the need to centralize command of cyber operations, which is the driving need behind the proposed establishment of USCYBERCOMMAND. Last is the need to further develop partnerships across the interagency and into the broader society and commercial sector (Departmemt of Defense 2010).

4. SELECTED ACTIONS TO MITIGATE SHORTFALLS

The authors of this paper believe that at least five recommendations should be implemented to mitigate existing shortfalls in the cyber force structure: education; higher education and recruitment; certification, retention, professional development and workforce management; exercises; and security clearance requirements. For

each of these recommendations, the following discussion characterizes the existing status and proposes recommendations to mitigate shortfalls.

4.1 EDUCATION

Currently, few public schools offer computer science courses due to lack of funding, qualified teachers, standards, and curriculum. Consequently, limited numbers of students study computer science at the high school or college level, and extremely few students enter the cyber workforce.

To mitigate this issue, it was recommended that we improve K-12 education. To implement this concept, we recommend that we provide formal training and set aside grants for K-12 instructors in computer science. In addition, it is important to institute standards for computer science in science, technology, engineering, and mathematics education and to make computer science courses available to middle and high school students. Although this recommendation does not directly affect the cyber pyramid, it provides the foundation for long-term cyber security.

4.2 HIGHER EDUCATION AND RECRUITMENT

Currently, Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) are dissatisfied with quality and quantity of computer security specialists.

With respect to *quality* they have observed that computer science programs are insufficiently staffed with qualified, experienced faculty. In addition, there is a significant disconnect between what universities are teaching and what the US government and private sector need.

With respect to *quantity* they have stated that educational institutions and the US government are not effectively recruiting talented youth for the cyber professions. Consequently, there is large base of potential talent that is not being tapped.

To deal with these issues, the authors propose the following recommendations. First, there is widespread support for the US Cyber Challenge and similar initiatives. The US Cyber Challenge is a national competition and talent search to find and develop 10,000 cyber security specialists (United States Cyber Challenge 2009). Three large-scale competitions are envisioned: CyberPatriot, for high school students, conducted by the Air Force Association; the Digital Forensics Challenge conducted by the DoD Cyber Crime Center (DC3); and the Network Attack Competition conducted by the SANS Institute. Second, there is interest in channeling interest through a variety of techniques including support through national competitions, internships,

scholarships and specialized training programs. As an example, House Resolution 4061 would create a cyber security scholarship program (Koss 2010). Third, there is interest in developing standards for teaching cyber security. Finally, we need to recruit top rate faculty and offer incentives to encourage them (e.g. fellowships).

Although the CNCI has stressed the importance of expanded cyber education, there are concerns that it has not been explicit in this initiative. The Government Accountability Office (GAO) recently issued a report on Cyber security that assesses the status of the CNCI (Government Accountability Office 2010). In that report they observe that "Stakeholders have not yet reached agreement on the scope of cyber security efforts". Consequently, they recommend that the Director of the Office of Management and Budgeting (OMB) "reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems."

Furthermore, as noted in (Associated Press 2010), the US military academies have increased their emphasis on cyberwarfare. At the US Military Academy at West Point, cyber security has been part of the curriculum taken by all students for years. Currently, information technology has been required for approximately ten years for all cadets who don't test out of the class. At the Air Force Academy, they have created an emphasis on the subject in 2004 by adding classes in cryptology, computer science, information warfare, and network security. Currently, every freshman at the Air Force Academy takes a class that includes some aspects of cyberwarfare. Since then, the school has graduated more than eighty students with an emphasis on cyberwarfare. Finally, the US Naval Academy Computer Science Department is running its first-ever cyber security course for students who are not computer science majors. Since December 2009, the Naval Academy created the Center for Cyber Security Studies. This activity is coordinated with the NSA and establishes a six-week internship program. In addition, they have created two new elective courses in computer science: Cryptography and Network Security and Computer Forensics.

4.3 CERTIFICATION, RETENTION, PROFESSIONAL DEVELOPMENT, AND WORKFORCE MANAGEMENT

The US government is not the most attractive employer (e.g. with respect to salary limitations). In addition, dynamic computer professionals often feel stifled and powerless in a large bureaucracy.

To address this issue, the authors believe that the following recommendations should be implemented. First, it is important to develop a cyber security talent management

plan that would serve to coordinate professional training and staffing needs. Second, there is interest in establishing exchange programs between the US government and the private sector. This would serve to educate members of the private sector so that they would understand the magnitude of the cyber security problem. Third, since the cyber security problem is continuing to evolve, it is important to have the US government support continuing education, certification, and development. Fourth, given the need to attract talented cyber security professionals, it is important to offer special hiring and pay authority. Finally, steps should be taken to employ the certification process so that it has a strongly rooted business case (Tipton 2009).

In the area of certification, the DoD has recently mandated that US Government cyber defenders must be able to perform "ethical hacking" (Montalbano 2010). The term "ethical hacking" was coined by IBM in the 1960s to define a way for IT security researchers to emulate the work of hackers so they can better defend networks. In a February 25, 2010 update to a directive on information security, DoD now requires its computer network defenders to pass Certified Ethical Hacker certification from the International Council of E-Commerce Consultants. This test is designed to explore the defender's ability to understand the mindset, tools and techniques of a hacker.

4.4 EXERCISES

The authors of this paper believe strongly that the US government must test how cyber security functions in a crisis. To that end, it is vital that all aspects of doctrine, organization, training, matériel, leadership and education, personnel and facilities (DOTMLPF) are assessed, holistically. In particular, realistic exercises must include the active participation of the private sector. We observe that typically, there is an overabundance of rules of engagement for conducting exercises that should be relaxed. In addition, it has been observed by the GAO that there has been a failure to incorporate lessons learned from exercises into the evolving DOTMLPF process (Government Accountability Office 2008).

To deal with those concerns, there is broad agreement that the US government must conduct "whole-of-government" exercises, including participation by the private sector at all stages of the exercise. It is vital that these exercises be realistic and that lessons learned are implemented across the interagency and the private sector. As an initial step, Lockheed Martin Corp and Johns Hopkins University's Applied Physics Laboratory have been awarded contracts by DARPA "to develop next-generation computer security testing systems against enemy cyber attacks" (Burnett 2010).

4.5 SECURITY CLEARANCE REQUIREMENTS

Currently, only a subset of graduating qualified computer professionals are clearable US citizens. Furthermore, the security process is long and expensive. Consequently, slots go unfilled or are filled by a person with lesser professional credentials but the right clearance level.

To deal with this issue, efforts should be made to hire more US citizens in the cyber workforce. Alternatively, efforts should be made to improve the clearance process (e.g. make it more efficient, more affordable, faster) or to institute more effective compartmentalization.

5. IMPLICATIONS FOR NATO

This paper has addressed the problems that the US faces in building a cyber force structure. The challenge of building a cyber force structure for NATO is beyond the scope of this paper and should be the subject of future research activities. However, many of the recommendations cited in this paper should be considered for application in the NATO context. These include: enhancements in lower and higher education; actions to improve the intellectual capacity of the cyber workforce (see Figure 2); steps to improve the planning, execution, and implementation of lessons learned for effective exercises; and the satisfaction of security clearance requirements. In addition, we believe that several of the initiatives in the CNCI should be broadened to address NATO cyber security issues (e.g. redirect Research and Development; develop leap-ahead technologies; develop cyber deterrence strategies).

6. SUMMARY AND RESIDUAL ISSUES

It is broadly acknowledged that current capabilities do not begin to satisfy cyber force needs. To mitigate these shortfalls, it is recommended that a *set* of actions should be taken. These include starting education early; improving higher education and recruitment; enhancing certification, retention, professional development, and workforce management; conducting and learning from more credible exercises; and paying additional attention to clearance requirements.

Overall, a coherent, consistent set of actions must be taken. This paper has also served to identify a set of issues that need to be addressed by senior decision-makers. In particular, senior decision-makers need to consider the following issues:

- Have the US Services adequately addressed career progression (note: many individuals in uniform are retiring and supporting cyber security as contrac-

tors)?

- Does NATO conduct realistic exercises and implement changes reflecting "lessons learned"?
- Should nations employ "patriotic hackers" (mirroring the perceived actions by the Russian government in their attacks against Estonia and Georgia (Bumgarner&Borg 2009))?
- What should be the role of the private sector and government organizations (e.g. the recent discussions between Google and the National Security Agency (NSA)) (Nakashima 2010b)?
- What steps can be taken to expedite the attribution problem?
- How should we refocus the Alliance's cyber deterrence posture?

REFERENCES

- Air Force Doctrine Center, 2008. Cyberspace Operations. Draft Air Force Doctrine Document 2-11, Maxwell AFB, AL, 2008.
- Associated Press, 2010. Cyberwarfare Gains Interest At Military Academies. Available at: http://wiz.com/local/Cyberwarfare.Military.2.1545372.html [Accessed March 8, 2010]
- Axe, D. Air Force Establishes 'Reduced' Cyber-war Command. *Danger Room* (August 18, 2009).
- Blair, D.C., 2010. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, February 2.
- Bumgarner, J., Borg, S., 2009. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008.* A US-CCU Special Report, August 2009.
- Burnett, R., 2010. Lockheed Training Unit Lands Deal to Make 'Cyber Range' for Next-Gen Security Software. *Orlando Sentinel,* February 3.
- Craft, J., 2009. Presentation to NDU Cyber Force Structure Conference, 29 October 2009.
- Department of Defense, 2010. Quadrennial Defense Review Report, February.
- Department of the Navy, 2009. *Cyberspace Policy and Administration Within the Department of the Navy,* SECNAV Instruction 3052.2, 6 March 2009.
- Deputy Secretary of Defense Memorandum, 2008. The Definition of Cyberspace. May 12.
- Fogelman, R., Widnall, S., 1995. *Cornerstones of Information Warfare.*
- Gates, R., 2009. *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations.* Memo, 23 June 2009.
- Gonzales, D., et al, 2005. *Network-centric Operations Case Study: Air-to-Air Combat with and without Link 16.* , RAND, Santa Monica, CA.
- Gosler, J., 2010. *Personnel communications,* January 2010.
- Government Accountability Office, 2008. *DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise.* GAO-08-825.
- Government Accountability Office, 2010. *Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative.* GAO-10-338.
- Koss, G., 2010. House Cyber security Bill Eases Toward Passage. CQ February 4.
- Kramer, F.D., Starr, S.H., Wentz, L.K., 2009. *Cyberpower and National Security.* Potomac Press, 2009.
- Marine Corps, 2003. *Air-Ground Task Force Information Operations.* Marine Corps Warfighting Publication 3-40.4, 9 July 2003.
- Marine Corps, 2010. *HQ MARFORCYBER Information Brief.* 25 January 2010.
- Montalbano, E, 2010. The Navy Becomes the Third Branch of the U. S. Military Military to Establish an Organization to Oversee Its Cyber security Activities and Protect Against Attack. *Information Week,* February 1, 2010.
- Montalbano, E., 2010. The Department of Defense mandate solidifies the practice of ethical hacking within its ranks of security pros. *Information Week*, March 2.
- Nakashima, E., Krebs, B., 2009. As Attacks Increase, U.S. struggles to Recruit Computer Security Experts. *Washington Post,* December 23.
- Nakashima, E., 2010a. FBI director warns of 'rapidly expanding' cyberterrorism threat. *Washington Post* March 4.
- Nakashima, E., 2010b. Google to Enlist NSA to Help It to Ward off Cyber attacks. *Washington Post,* February 4.
- NRC, 2010. *NRC Prize for Cyberdeterrence Research & Scholarship.* [Accessed March 11, 2010] Available at: http://sites.nationalacademies.org/CSTB/CSTB_056215

- Owens, W.A., Dam, K.W., Lin, H., 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities.* National Research Council.
- The United States Cyber Challenge, US Cyber Challenge Version 1.1, May 8, 2009.
- Tipton, W.H., 2009. DoD Certifies the Power of Partnership. *IAnewsletter*, Volume 12, November 4.
- Training and Doctrine Command, 2010. *TRADOC Pamphlet 525-7-8: The US Army's Cyberspace Operations Concept Capability Plan, 2016-2028.* Fort Leavenworth, KS: 22 February 2010.
- Webber, R., 2009. *NDU Cyber Force Structure Conference.* 29 October 2009.

GLOSSARY

Abbreviation	Meaning
ADM	Admiral
CAC	Combined Arms Center
CBA	Capabilities-Based Assessment
CCP	Concept Capability Plan
CWID	Coalition Warrior Interoperability Demonstration
CONOPs	Concept of Operations
DARPA	Defense Advanced Research Project Agency
DHS	Department of Homeland Security
DIRNSA	Director, NSA
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
EMS	Electro Magnetic Spectrum
ICANN	Internet Corporation for Assigned Names and Numbers
INSCOM	Intelligence and Security Command
JFCC-NW	Joint Functional Component Command for Network Warfare
JTF-GNO	Joint Task Force – Global Network Operations
K	Kindergarten
MacForCyber	Marine Forces Cyber
MAGTF	Marine Air Ground Task Force
MCNOSC	Marine Corps Operations Support Center
NATO	North Atlantic Treaty Organization
NDU	National Defense University
NETCOM	Network Enterprise Technology Command
NRC	National Research Council
NSA	National Security Agency
QDR	Quadrennial Defense Review
SACEUR	Supreme Allied Commander Europe
US	United States
USA	United States Army
USAF	United States Air Force
USMC	United States Marine Corps
USN	United States Navy

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

PINPRICK ATTACKS, A LESSER INCLUDED CASE?

Antoine LEMAY[a,1], José M. Fernandeza, Scott Knight[b]

[a]*École Polytechnique de Montréal, Montreal, Canada,*
[b]*Royal Military College, Kingston, Canada*

Abstract: Defense has always been tailored to threats; this prevents wasteful resource spending and strategic surprise. However, with the introduction of asymmetric warfare techniques, including cyberwarfare, defending against all threats has become impossible. To deal with this problem, the notion of "warfare spectrum" was introduced. At one end of the spectrum stands complete peace, at the other end high-intensity kinetic warfare. The theory behind this was that a force trained for high-intensity would be able to deal correctly with "lesser included cases" in the spectrum. This way of thinking has also been applied to cyberwarfare and critical infrastructure defense.

In the literature, we can notice a definitive focus on preventing a "cyber Pearl Harbor" or "cyber 9/11", meaning an unforeseen, devastating attack. Alternatively, following the events in Georgia and Estonia, the protection from massive coordinated denial of service was also considered. Still, both of these scenarios sit in the high-intensity spectrum of cyberwarfare. However, in our analysis, we have found that low-intensity cyberwarfare could be as devastating and cannot be considered a "lesser included case" of high-intensity cyberwarfare, contrary to what the "warfare spectrum" theory dictates. In particular, we present the "pinprick attack" scenario, where the goal of an attacker is to produce long-term damage by the accumulation of large numbers of low damage attacks.

In our paper, we demonstrate why new solutions are needed to defend against our scenario. First, we illustrate how a "Clausewitzian" definition of warfare limits the kind of responses that are available to the target of such an attack.

1 École Polytechnique de Montréal, 2500 chemin de Polytechnique, Montréal, H3T 1J4, Canada, Email: antoine.lemay@polymtl.ca.

Because no formal declaration of war is made, responsibility for defense will rest on the private sector and not military institutions. Then, we see that existing defense solutions, such as data aggregation by national agencies and generalized vulnerability reduction, fare poorly against the pinprick attack scenario because the damage threshold is kept small and because the attack's breadth is very large. Finally, we present some ideas to counter "pinprick attacks". Notably, we mention the optimization of defensive solutions to cover a wider range of threats (our own research project) and regulatory economics (field for future work).

Keywords: cyber warfare, asymmetric warfare, critical infrastructure protection

INTRODUCTION

Defense has always been tailored on threats; this prevents wasteful resource spending and strategic surprise. However, with the introduction of asymmetric warfare techniques, including cyberwarfare, defending against all threats has become impossible and defenses are focused on likely threats. This leaves holes that can be exploited by new attack forms. In particular, we will analyze how the assumption that a cyberwarfare opponent would use a high-intensity form of cyberwarfare creates holes where a low-intensity form of cyberwarfare can thrive.

We will start by looking at how governments plan to solve the cyber security problem of critical infrastructure. This will allow us to extrapolate the attack scenarios that are considered high threat. We will then compare this scenario with current military thinking in order to confirm our extrapolation. We also analyze the limitations inherent to the scenario. Finally, we present an attack form, the pinprick attack, which uses these limitations to maximize the damage it can cause and we offer avenues for future research that would enable defenders to defeat our attack.

1. CRITICAL INFRASTRUCTURE PROTECTION

A lot of effort has been invested to bolster cyber security. A group of experts mandated by the Center for Strategic and International Studies (CSIS) argued again in 2008 in their Cyber Security for the 44th Presidency report that "cyber security is now a major national security problem for the United States" (CSIS, 2008). Within that major national security problem lays the problem of securing critical infra-

structure against attack. Various solutions have been proposed to reduce the risk associated with cyber attacks on the critical infrastructure. However, these solutions are based on unconscious strategic assumptions that might prove not to be true.

In this section, we will look at the two most common propositions to reduce cyber security risks on the critical infrastructure. We then analyze the solutions to extract the scenarios they are most useful against. Based on this analysis, we draw conclusions about the strategic assumptions that drive the efforts to reduce risk.

1.1 VULNERABILITY REDUCTION

The most common solution to reduce the risk for the critical infrastructure is some sort of vulnerability reduction program. The 2003 National Strategy to Secure Cyberspace has two national priorities addressing this issue. Priority II (a national cyberspace threat and vulnerability reduction program) addresses technical vulnerabilities while Priority III (a national cyberspace security awareness and training program) addresses human vulnerabilities (Department of Homeland Security [DHS], 2005). Various methods have been employed to attain these goals. One example of vulnerability reduction program is the North American Electric Reliability Commission (NERC) Critical Infrastructure Protection (CIP) standards (NERC, 2010) that are required to be met by January 2010. The idea behind this strategy is that once vulnerability has been reduced, an opponent will not have any opportunity to attack.

The underlying assumption behind the concept of generalized vulnerability reduction is that it is possible to reduce your vulnerability enough to make attacking you inefficient. It is clearly not possible to reduce the vulnerability over the entire attack surface. As Welander shows in his review of cyber security for the industrial control sector (Welander, 2009), skilled and motivated attackers, such as spies and extortionists, tend to use more sophisticated attack strategies. In particular, highly committed opponents can afford to use a strategy of systematic probing for vulnerabilities. In fact, they can also attempt to induce vulnerability in the target by finding undisclosed vulnerabilities or by distributing Trojan horses or backdoors for example. As skill and motivation increase, it becomes increasingly costly to reduce vulnerability to a point where no risk exists. In that light, the implied objective of national vulnerability reduction programs is to address the lower left quadrant of Figure 1, i.e. widely known vulnerabilities affecting your industry in general. This is even truer if the private sector is to assume the costs of vulnerability reduction as in the case in NERC CIP standards. Because the private sector is profit-driven and has no vested interest in national security, market forces will drive the private sector to minimal compliance. That minimal compliance will be aimed at defeating casual

attackers, which is possible to do at reasonable costs, and not highly trained and motivated attackers, which are an unlikely threat and very costly to defend against.

1.2 DATA CORRELATION

The other solution that is most often proposed is the creation of a national agency to collect and correlate data. This can take various forms. For example, in the Department of Homeland Security (DHS) report on the National Strategy to Secure Cyberspace, Priority I is a "National Cyberspace Security Response System" (DHS, 2003). In the report for the 44th Presidency, the authors ask that the president "reinvent the public-private partnership" (CSIS, 2008). This is usually done by the creation of Computer Emergency Response Teams, or CERTs as described in the DHS press release detailing its activities in regards to the National Strategy to Secure Cyberspace (DHS, 2005). Once established, the CERTs share information with the various government agencies and the private sector. The idea being that the global situational awareness obtained through the centralization of information and the established relations with various actors will allow the CERT to successfully coordinate efforts to diffuse a crisis. This model is widespread even if only US sources are presented. We can find CERTs in the US, in Canada, Australia, Estonia and even in non-NATO countries such as Russia.

If one assumes that the CERT model works as designed (and the various improvements suggested in the report to the 44th Presidency suggest that it may still require improvement), the CERT model itself is based on a critical assumption. It is assumed that centralization of data will produce an increased situational awareness that can be turned into a defensive advantage. The only scenario where that assumption is likely to prove correct is in the case of a concerted effort by an attacker to target a variety of CERT partners. For example, an opponent coordinating DoS attacks on government servers, banks and television networks would be able to be easily correlated by a CERT and actions could be taken to deal with the situation as a whole instead of in isolation. However, in order to make such a correlation, it is necessary to have some sort of link between the attacks such as a temporal link (e.g. after a political event). Other types of linkage are possible, but may not enable a CERT to produce a coordinated defense. For example, a series of attacks using the same methodology over a long period of time could be eventually correlated, but it would likely be too late for a response.

1.3 STRATEGIC ASSUMPTIONS

As we have seen, proposed solutions to reduce the risk to critical infrastructure are

based on specific risk scenarios. In the case of vulnerability reduction, we want to reduce the exploitation of low hanging fruits vulnerabilities by unskilled attackers. In the case of centralized data correlation, we hope to be able to detect and respond to correlated attacks. This kind of attack footprint can be associated with a limited number of strategic scenarios.

The first scenario is the asymmetric opponent. In this scenario, an opponent decides to target your infrastructure with a massive cyber attack to make you hurt as much as possible. This can be used as a support for deterrence much in the same way as other asymmetric warfare tactics (e.g. insurrection) are attempted. The attacks in this scenario are performed by an inferior opponent. They are likely to be limited in terms of skill because of the limited resources that can be deployed by the inferior opponent who may not possess highly trained assets that can exploit less widely known vulnerabilities or does not have a large amount of time to induce vulnerabilities or perform exhaustive vulnerability searches. Also, the attacks are likely to be correlated in time (linked with specific deterrence event) and space (originating from the same region). Similarly, coordinated effort is likely to be worthwhile because of the high correlation.

The second scenario is the use of cyberwarfare to support military operations. The most common example is the use of cyberwarfare to perform command and control warfare. In that example, the cyber attacks are heavily correlated in time (with conventional warfare operations) and targeting (command and control assets). Response can also be easily centrally coordinated as part of a military response. Because it is linked with military operations, a high tempo can be expected. In that sense, limited use of exhaustive vulnerability research and research for new vulnerabilities is not likely to happen once operations start. In that sense, the attack footprint would be similar to the asymmetric opponent scenario.

In both of these cases, we are dealing with a clear opponent and a high tempo of cyber attacks. As such, both of the scenarios can be considered high-intensity cyberwarfare. But are there low-intensity cyberwarfare scenarios?

2. INTENSITY IN CYBERWARFARE

Based on the solutions that are proposed to reduce the risk for critical infrastructure, one might extrapolate that our main concern is high-intensity warfare scenarios. In this section, we see how this fits conventional western military thinking and the limitations of this view.

2.1 WARFARE SPECTRUM

Western military doctrine is significantly influenced by the works of Von Clausewitz. In particular, that war is the continuation of politics by other means. This led to the development of the "spectrum of warfare", described in various doctrine documents such Canada's Army (National Defence Canada, 1998) and Land Operations (National Defence Canada, 1998). Figure 1 illustrates the concept.

As we can see, operational military means are only employed in times of conflict or war. In that mindset, it is normal that cyberwarfare would be employed in the same conditions. These conditions dictate how force is used, even for cyberwarfare. In a condition of war, the goal is usually to bring a quick end to the conflict. As such, there is no incentive to limit the damage you are doing to the enemy. This is consistent with the attack profiles for high-intensity cyberwarfare presented earlier.

Because of the dangerous nature of the warfighting end of the spectrum, modern armed forces are trained first and foremost to deal with combat operations. The rationale is that if you are trained for the difficult, you will excel at easier tasks.

<table>
<tr><th>Peace</th><th>Conflict</th><th>War</th></tr>
<tr><td colspan="2">Military operations other than war</td><td></td></tr>
<tr><td colspan="2">Strategic military response</td><td>Warfighting</td></tr>
<tr><td colspan="2">Non-combat operations</td><td></td></tr>
<tr><td>Operational military means</td><td colspan="2">Combat operations</td></tr>
</table>

Figure 1. Spectrum of warfare

This is confirmed by Canadian doctrine. In the Land Operations publication (National Defence Canada, 1998) we read that "combat capable forces are flexible enough to adapt to the requirements of **non-combat operations**" (original emphasis). In other words, non-combat operations are lesser included cases of combat operations. By following this thinking in cyberwarfare, it makes sense to concentrate on defending for high-intensity cyberwarfare.

2.2 LIMITATIONS

The main limitation of the traditional western military thinking is that military response is not triggered until the conflict has been escalated. Typically, some sort of declaration of war or act of war is required. In the cyberwarfare world, this would require a successful correlation of the attacks before committing to an organized

response. If the correlation cannot be made, the defense framework that is in place (e.g. CERT teams, government agencies, etc.) cannot be used. Also, because time is one of the primary factors that drive attack correlation, low-intensity warfare is unlikely to be successfully correlated as "warfare". This is not a problem when dealing with other nations that are following the same set of principles for warfare and politics, but can become a problem when dealing with countries (or organizations) that do not.

The intense competition between classical Chinese states as illustrated in Chinese military classics (Sun Tzu (2006) and Sawyer (1993)) offers a great example of a diverging theory for what constitutes warfare. Everything your state gains at the expense of other is ultimately a strategic advantage that you will be able to use later and thus is, in essence, warfare. This way of thinking is still present in modern Chinese military literature. For example, in the book "Unrestricted Warfare", Liang and Xianshui (1999) argue that multiple forms of warfare such as financial warfare, trade warfare and cyberwarfare could play a major role in wars of the future. Obviously, the role of these alternate forms of warfare is to diminish the fighting strength of a nation by attacking the national assets that support the military establishment. Naturally, no nation would allow itself to be attacked in that fashion.

This leads to another limit on the concept of high-intensity cyberwarfare. There are inherent limits to the damage you can cause to any opponent that has the means to defend itself. The first limit is the ability for the target to "pull the plug" or disconnect his network from yours. Even the Internet requires a backbone, which can be deliberately partitioned by cutting a limited number of points (for example the endpoints of oceanic cables (Internet's Undersea World, 2010)). So, if you are facing a rational opponent, the damage he can inflict on himself by pulling the plug (and whatever you can sneak in before he does) is the upper bounds to the damage you can inflict. If he assesses that you can do more damage to him than the damage of pulling the plug, he will disconnect, and if you can't he will accept your damage. The second limit is the ability for the target to escalate. To illustrate, let us consider what would be the US response to an enemy trying to disable a vital strategic asset such as the US nuclear command and control system. We can easily extrapolate that this would provoke a significant response using a broad spectrum of means.

By taking a low-intensity approach, it is possible to abuse these limitations to create a new cyberwarfare threat.

3. PINPRICK ATTACKS

Pinprick attacks are an illustration of what can be done with low-intensity cyber-

warfare. With Pinprick attacks, the trick is for the attacker to lead the defender into believing he is facing unconnected single instances of small attacks. This is done by staying under his correlation threshold. It is similar to the practice of "slow slicing" or "death by a thousand cuts" in the sense that you do not perform a single crippling attack, but instead a collection on non-crippling attacks whose effects add up to create the crippling effect.

3.1 DESCRIPTION

In our pinprick attack scenario, individual damage per incident is low. It is therefore ill suited to attack hardened targets built with resilience in mind such as military communications. However, because it is a long-haul strategy, we can perform attacks on select points which will yield good results. The specific targeting of ball bearing factories by US bombers in World War II is an example of operations designed to destroy a fighting capability without actually directly targeting military hardware. Can such an operation be carried out in a cyberwarfare context? RAND's publication "Measuring National Power in the Postindustrial Age" (Tellis et al, 2000) offers us some insight into how this could be done. This report presents a methodology to evaluate a nation's power using more than military power as the sole criterion. In the RAND model, combat proficiency is a result of the combination of strategic resources and the capability to convert these resources into military power. The easiest example is the case of military technology. A country with rich resources into terms of knowledge and money (strategic resource) can transform this resource in military technology through its military-industrial complex (conversion capability). Because we are talking about a combination, affecting either the resources or the conversion capability will result in a decrease in military power. We could present our "death by a thousand cuts" scenario as gradually injecting grains of sand into a complex clockwork mechanism in order to make it stop, or at the very least run less efficiently.

Defense from this scenario, in western countries, is mostly under the control of the private sector. For example, privately owned banks control most of the financial system, privately owned power companies supply the power, privately owned companies produce most of the technology and hardware used by the military. The goal of these companies is to make profit. This objective is usually incompatible with spending money to defend against an unlikely scenario (e.g. cyberwarfare). Increased spending for cyber security can even be detrimental to the health of a company. After all, if your costs are higher than those of your competition because of high security measures, customers will buy your competitor's products. This breeds a vulnerability-rich environment that drives the costs of creating an attack operation down even in the face of government-mandated vulnerability reduction

programs. Attackers have all the time they need to perform exhaustive searches for vulnerabilities because the attack follows a deliberately slow tempo. This gives a determined attacker the agility required to attack only targets of opportunities and to follow the path of least resistance and pick the low hanging fruits. In that sense, a vulnerability reduction program does not offer adequate protection against pinprick attacks.

An important aspect of pinprick attacks is to keep the defender unaware that the attacks he is seeing are part of a coordinated strategy. As long as he is not able to correlate the attacks, there is no theoretical limit to the amount of damage you can inflict. This can be explained by the fact that, compared with each incident in isolation, the cost of coordinated response will always be higher than the incident's damage. For example, if you find a Trojan horse on a military contractor's computer, you clean it and try to assess the damage. If you find one on someone else's computer the next week, you will do the same. However, if you find a Trojan on the computers of all the military contractors, you might take more active measures to stop whatever is going on. So, by design, pinprick attacks are difficult to defend against by centralized data correlation agencies such as CERTs.

3.2 EXAMPLE

Because pinprick attacks reside in the low-intensity part of the spectrum, they are not well suited for what we consider warfare scenarios, which require speedy conflict resolution. However, it is ideally suited for competition between near peers where one of the peers wants to slow down the progress of his other peers to catch up with them or increase its advantage.

Let us consider the fictional scenario where the countries of Alpha and Beta are near peers. However, the people of Alpha possess a significant advantage in technology over Beta. This advantage in technology allows the military of Alpha to hold a strategic advantage over Beta's military force, even if both are similar in other aspects. If Beta were to pursue a high-intensity cyberwarfare strategy, Alpha could respond by pulling the plug and escalating to a military conflict where Alpha has the advantage. This course of events is therefore detrimental to Beta. However, Beta can instead decide to be patient and use pinprick attacks, slowly but methodically launching attacks to undermine the confidentiality around Alpha's technology. Beta can sum up the benefits of all his attacks (plans captured by a Trojan, information recovered from a stolen USB key, communications intercepted on the wire, etc.) to catch up with Alpha in technology and negate Alpha's strategic advantage. It is unlikely that Alpha would recognize that the various incidents are connected to a coordinated effort by Beta to negate a military advantage because individual incidents only cause limited damage.

3.3 COUNTERING PINPRICK ATTACKS

As we have seen previously, the solutions that are currently proposed to deal with cyber threats are not really appropriate to deal with pinprick attacks. In order to defend effectively against them, new solutions are required.

The ideal solution would be to possess the means to correctly correlate attacks, but this is very difficult. After all, the attacker can set the tempo to whatever value allows him to evade detection (although there is admittedly a value under which the tempo would be too low to produce significant damage). We must therefore concentrate on vulnerability reduction. Again, as we have seen, this can also be a daunting task. However, unlike correlation, defenders have the levers of technology and economics to tackle the problem. In both cases, the goal is not to completely reduce the vulnerability, but instead to reduce the damage to the investment ratio of the attacker.

This can be achieved by having better technology. If, with the same market constraints, we can provide better security, we will blunt the attacker's advantage. If we manage to build security devices that are cheaper, implementing adequate security will prove less of a burden on the private sector. It will then be possible to ask more security of the private sector. Similarly, finding ways to optimize the efficiency of existing technology is another avenue that can be pursued. In particular, finding ways to use existing technology to extend the threat coverage could prove to be an interesting field of research in that regard.

The other option to increase the overall security is to change the market constraints. A tool governments have at their disposal is regulatory economics, e.g. by providing subsidies to critical infrastructure operators to upgrade their security. Another example would be the creation of penalties if some level of security is not achieved as is the case in the NERC CIP standards (NERC, 2010). While our research group is not focused on economics, this field could prove to be fruitful for further research.

4. CONCLUSION

In this paper, we have analyzed the solutions that are more commonly proposed to deal with the cyber security of the critical infrastructure. In particular, we have seen that national programs of vulnerability reduction are mostly successful in reducing the vulnerabilities used by unskilled attackers. As for centralized correlation of data, we have seen that it requires distinguishable patterns in the attacks to be successfully correlated. More importantly, we argued that successful correlation is required for a coordinated defense. These limitations reveal the underlying assumption that

the expected opponent will use some form of high-intensity cyberwarfare. While that assumption is reasonable for an opponent following a military doctrine based on von Clausewitz's writings, we cannot assume that all opponents would adhere to such a philosophy.

To prove that low-intensity cyberwarfare is possible, we have proposed the "pinprick attack" scenario where an opponent launches a series of attacks too small and too distant to be successfully correlated. Because the attacks cannot be correlated, a nation cannot offer a coordinated response such as escalating the conflict to a field more advantageous for the defender, such as conventional warfare, or such as "unplugging" from the network. The attacker can then endlessly repeat his attacks to cause a "death by a thousand cuts".

Because current defensive strategies are not well adapted to deal with pinprick attacks, future work is required to bolster defenses. In particular, research to reduce the financial burden of security for critical infrastructure operators is an avenue that our research group pursues. Another promising avenue of research would be the use of regulatory economics to change the market forces that drive the critical infrastructure operators to the lowest common denominator.

REFERENCES

- Author unknown, 2010. *The Internet's Undersea World.* Internet: http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg, [Feb. 2010]
- CSIS Commission on Cyber Security for the 44th Presidency, 2008. *Securing Cyberspace for the 44th presidency.* Internet: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, December 2008 [Feb. 2010]
- Department of Homeland Security, 2003. *The National Strategy to Secure Cyberspace.*
- Department of Homeland Security, 2005. *Fact Sheet: Protecting America's Critical Infrastructure – Cyber Security.* Internet : http://www.dhs.gov/xnews/releases/press_release_0620.shtm, Feb. 15 2005 [Feb. 2010]
- Liang, Q. and Xianshui, W., 1999. *Unrestricted Warfare.* PLA Literature and Arts Publishing House
- National Defence Canada, 1998. *Canada's Army.*
- National Defence Canada, 1998. *Conduct of Land Operations.*
- North American Electric Reliability Commission, 2010. *Critical Infrastructure Protection standards.* Internet : http://www.nerc.com/page.php?cid=2|20, [Feb. 2010]
- *T'ai Kung's Six Secret Teachings* in Sawyer, R. D., 1993. *The Seven Military Classics of Ancient China.* Westview Press, USA.
- Sun Tzu, 2006. *The Art of War.* translated by Griffith, S. B., Blue Heron Books, Canada
- Tellis, A. J. et al, 2000. *Measuring National Power in the Postindustrial Age.* RAND, USA.
- Welander, P., 2009. *Cyber Security.* Control Engineering, vol. 56, no 1, January 2009, p. 41.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

STATE RESPONSIBILITY FOR CYBER ATTACKS: COMPETING STANDARDS FOR A GROWING PROBLEM

Scott J. SHACKELFORD[a,1]

[a]*University of Cambridge, Cambridge, UK*

Abstract: This Article reviews both the applicability and desirability of the two vying regimes for state responsibility under international law as applied to cyber attacks: the effective and overall control standards. Due to the technical difficulties with proving attribution for cyber attacks, along with the unreasonably high burden of proof required by the ICJ's interpretation of the effective control standard, this Article argues for the adoption of the overall control standard as being both within the best interests of NATO as well as the international community.

Keywords: state responsibility, cyber attacks, international law, NATO, cyber security

1 Department of Politics and International Studies, University of Cambridge, 17 Mill Lane, Cambridge, CB2 1RX, UNITED KINGDOM, Email: ss645@cam.ac.uk.

INTRODUCTION

At a time in which the unchecked sovereign authority of States is being challenged across many arenas, State responsibility remains a key bulwark of international security (Held, 2006, p. 293-97; Reich, 1991). But constructing a viable regime to define State responsibility in international law has proven to be elusive. Instances of State-sponsored terrorist acts have increased since the end of the Cold War, but proving State responsibility for such acts remains exceedingly difficult (Brenner & Crescenzi, 2006, p. 398; Burgess 2006, p. 302; Joyner & Rothbaum, 1993, p. 229). This problem is magnified in cyberspace by the speed and anonymity of cyber attacks, making according to the White House "distinguishing among the actions of terrorists, criminals, and nation States difficult." (*National Strategy to Secure Cyberspace,* 2003, p. 19 & p. 64). As seen in the 2007 cyber attack on Estonia, a potential sponsoring State may not cooperate in the investigation, apprehension, and extradition of those who committed criminal or terrorist acts on its behalf (Davis, 2007). Given the clandestine nature of cyberspace, States may thus incite civilian groups within their borders to commit cyber attacks and then hide behind a, however sheer, veil of plausible deniability and thus escape accountability.

This Article analyzes the two primary legal regimes of State responsibility for cyber attacks that could mitigate such State sponsorship: the effective and overall control standards. In brief, the effective control doctrine, originating in the International Court of Justice (ICJ) *Nicaragua* case, recognizes a country's control over paramilitaries or other non-State actors only if the actors in question act in "complete dependence" on the State (Nicaragua v. United States, 1986, p. 110). In contrast, the overall control doctrine, illustrated in the International Criminal Tribunal for the Former Yugoslavia *Tadic* case, held that where a State has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control such that the group's acts are attributable to the State (Prosecutor v. Tadic, 1995). This Article argues for the adoption of the latter standard of State responsibility for cyber attacks given the extreme technical difficulties involved with proving the identity of cyber attackers.

The Article is structured as follows. Part I constitutes a brief literature review on the question of appropriate standards of State responsibility for cyber attacks, taking special note of the unique scholarly contribution of this Article. Part II summarizes some of the myriad technical challenges raised by tracing cyber attacks. Part III discusses the fundamental problem of attribution as well as the cases for and against the effective and overall control standards of State responsibility for cyber attacks. Finally, Part IV demonstrates how defining State responsibility is critical within the context of NATO's cyber security strategy.

1. LITERATURE REVIEW HIGHLIGHTING ORIGINAL CONTRIBUTION

The literature to date has only obliquely dealt with the issue of State responsibility for cyber attacks in international law. Some works note that armed coercion is generally chargeable to States more so than other forms of coercion, but do not address the degree of proof needed to constitute State responsibility (Schmitt, 1998, p. 885). Other articles adopt *Nicaragua's* framework as applied to non-State actors, but not necessarily States (Schapp, 2009, p. 145). Much of the rest of the existing scholarship focuses on cyber terrorism by non-State actors, such as Verton (2003) or Ryan (2007). The one recent collection of essays on cyber warfare entirely ignores the topics of State responsibility, attribution, sovereignty and management of the information commons, all of which are central to countering cyber attacks (Janczewski & Colarik, 2008). There is thus a paucity of literature dealing with cyber attacks from the lens of international law and relations, to say nothing of the ethical and human rights implications of cyber attacks on national and international security (Wolf, 2000, p. 95; Yang, 2006, p. 201). Treatments of cyber attacks and information warfare outside the orthodox international humanitarian law framework are also nearly non-existent (Hanseman, 1997, p. 173). In particular, the literature to date has been silent on the appropriate legal regime to use as a baseline for regulatory responses to cyber attacks despite the fact that a developed system of treaties on the law of war now governs many aspects of the conduct of modern warfare, from weapons of mass destruction to the treatment of POWs and non-combatants.[2]

Nor has the growing literature on the rise of Internet law and the information commons applied its findings to the question of State responsibility for cyber attacks (Hunter, 2003; Johnson & Post, 1996, p. 1367; Lessig, 1999, p. 500). Even those recent works that do address cyber attacks and critical infrastructure protection do so primarily from a U.S.-centric vantage point, such as Cordesman (2002), or Lulasik (2003). Consequently, there is an important gap in the international law literature that this work addresses by explicitly laying out the cases for and against each potential regime of State responsibility for cyber attacks, analyzing the relative strengths and weaknesses in the context of NATO operations, and making a case for the adoption of the overall control standard. Before the respective options for State responsibility are examined though, first a brief introduction of the technical challenges of tracking cyber attacks is warranted.

2 The United States, for example, is party to eighteen law-of-war treaties. For a survey, see U.S. Department of State, Treaties in Force, 2007, *available at:* http://www.state.gov/s/l/treaty/treaties/2007/index.htm.

2. A BRIEF SUMMARY OF THE SCIENCE OF TRACING CYBER ATTACKS

The science of tracing cyber attacks is primitive at best. Sophisticated attacks by knowledgeable hackers, whether private or State-sponsored, are nearly impossible to trace to their source using modern practices (Lipson, 2002). The current foundation of network communications in cyberspace, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), dates back to 1982 (Lipson, 2002, p. 5). It is this antiquated system of communication designed for a small number of academic and governmental researchers sharing information with low risks of system breaches, which is at the heart of the problem for tracing cyber attacks (Lipson, 2002, p. 14). Though, of course, this is not the only problem—system vulnerabilities are multiplied when considering the myriad problems with often rushed to market commercial off-the-shelf software. Other issues include the facts that: the Internet was never designed to track or trace users, or to resist untrustworthy users; a packet's source address itself is untrustworthy and is easily masked; the current threat environment in cyberspace exceeds the Internet's design parameters; and there are myriad strategies that hackers employ making tracking difficult, such as tunneling and the destruction of data logs. But the overarching issue is that the current system was designed for a small number of trustworthy and tech-savvy researchers, which is simply no longer the case with more than a billion Internet users worldwide (Internet: *General Usage Statistics,* 2003).

Can the cyber infrastructure be modernized to enhance security and stop cyber attacks once and for all? The short answer is yes, but not easily. Certain strategies pioneered by the U.S. Cyber Emergency Response Team (USCERT) are promising, such as the use of probabilistic traceback techniques to audit a small percentage of packets so as to find the source of major distributed denial-of-service (DDoS) attacks of the kind that Estonia suffered in March 2007 (Hughes, 2009). There is also the possibility of tracing back single IP packets, though this is much more difficult (Lipson, 2002, p. 27). A full review of the myriad technical issues and their potential solutions is beyond the scope of this Article. Suffice it to say though, ultimately these technical countermeasures will never offer a complete solution to the problem of cyber attacks. Cyberwarfare is an arms race that cannot be won by defense alone. In the end, these attacks will likely continue to proliferate both in numbers and severity; the question then is how best they should be dealt with in international law and relations.

3. THE FUNDAMENTAL ISSUE OF ATTRIBUTION AND THE CASE FOR THE OVERALL CONTROL STANDARD

Attribution of a cyber attack to a State is a, if not *the*, key element in building a functioning legal regime to mitigate these attacks. The laws of war requires one State to identify itself when attacking another State, though this convention is honored more in the breach than in compliance (Brenner, 2006, p. 398; *The Hague Convention Relative to the Opening of Hostilities*, 1910, art. I). When there is a question about State sponsorship of aggression, two competing standards for State responsibility now exist in international law under Article VIII of the International Law Commission's Draft Articles on the Responsibility of States for International Wrongful Acts. Article VIII implicates State control when State actors or official organs are acting under the direction of the State (*Responsibility of States for Internationally Wrongful Acts*, 2001). An exact definition of 'control,' however, has been left up to the courts to interpret. The first standard that the courts have created is the ICJ *Nicaragua* effective 'operational control' standard (Nicaragua v. United States, 1986, p. 392). *Nicaragua* requires that a country's control over paramilitaries or other non-State actors can only be established if the actors in questions act in "complete dependence" on the State. The second standard is the ICTY *Tadic* 'overall control' standard. The ICTY held that where a State has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control, and the group's acts are attributable to the State (Prosecutor v. Tadic, 1995, para. 70). In so finding, the majority interpreted the decision of the ICJ in *Nicaragua* as requiring the government of a State to exercise "effective" control over the operations of a military force in order for the acts of that force to be imputed to the State (Pronk, 1997).

The most recent case in which the ICJ reviewed the competing standards of State responsibility was the *Application of the Genocide Convention ("Bosnian Genocide").* There, the Court adopted the effective control rather than the overall control standard in deciding that Bosnia lacked the specific intent to commit genocide (Bosnia and Herzegovina v. Serbia and Montenegro, 2007; Cassese, 2007). In essence, the Court required "smoking-gun" evidence or its equivalent (Luban, 2007, p. 30). The standard laid down by the Court was beyond *any* doubt, not beyond a *reasonable* doubt. This distinction is significant enough to potentially have been dispositive of the case's outcome, just as it is for holding State sponsors of cyber attacks accountable. Future cases will also likely turn on this distinction, necessitating an in depth analysis of the benefits and drawbacks of each standard for State responsibility.

3.1 THE CASE AGAINST THE EFFECTIVE CONTROL STANDARD

As a result of the divergence in international law on the issue of State responsibility, there are two competing standards emerging for cyber attacks: the effective control standard applicable to non-State actors, and both the effective and overall control standards applicable to State sponsors of cyber attacks. For non-State actors, the ICJ held in *Nicaragua* that effective control was the appropriate standard to apply at least in the paramilitary context of that case (Capaldo, 2007, p. 104). If this decision were to be extended to cyber militia, it would mean that the only instance in which State sponsors of cyber attacks would be held accountable for their involvement would be if their effective control could be proven beyond *any* doubt. Given what has been demonstrated about the extreme technical difficulties of proving the identity of cyber attacks due to the nature of the Web's architecture, such a standard would in essence give a free pass to State sponsors of cyber attacks. In a sophisticated global cyber attack, missing or corrupted data commands may be sufficient to disprove State control and defeat accountability. Without either new techniques such as the probabilistic tracing project mentioned in Part II, or very unsophisticated hackers, effective control would make State responsibility for cyber attacks virtually a non-starter.

There are other important drawbacks to adopting the ICJ's *Nicaragua* formulation with regards to proving State responsibility for cyber attacks, among them being the fact that the Court divided the use of force into "most grave" and "less grave" categories (Nicaragua v. United States, 1986, p. 101). This distinction has split commentators. Some see this view as formalistic and restrictive, and according to Gray (2000, p. 141) it "will encourage aggression of a low-key kind." Others see a low threshold of armed attack mixed with collective self-defense as a recipe for the internationalization of civil conflicts (Watkin, 2004, p. 5). As applied to cyber attacks, this doctrine could arguably give low-level cyber attacks, potentially up to and including the cyber attacks on Estonia, a pass at least as applied to international humanitarian law. This could encourage criminals, if all they have to worry about is law enforcement, and not the armed forces. Instead, and while the law of cyberwarfare remains malleable, the overall control standard should be adopted.

3.2 THE CASE FOR THE OVERALL CONTROL STANDARD

The ICJ has consistently used the more restrictive effective control standard in its jurisprudence, most recently in *Bosnian Genocide*, but other tribunals, such as the

ICTY, have not. Judge Antonio Cassese, the first President of The Hague Tribunal, attacked the B*osnian Genocide* judgment as demanding an "unrealistically high standard of proof" (Tosh, 2007). This burden of proof is nearly impossible to satisfy in the context of cyberspace without major improvements in the tracing of cyber attacks. As a result, if international law is to have sufficient applicability to cyberwarfare, it is essential that the overall control standard be adopted as part of a future international regime for cyberspace. Currently the framework for how such a treaty would operate is being debated, for the first time, by representatives of the United States and Russia. The two sides are far apart, but even preliminary discussions are encouraging (Markoff & Kramer, 2009). If these talks do bear fruit, their scope should be expanded to formulate a standard of State responsibility for cyber attacks.

Short of a new treaty on cyberspace, and alternatively to adopting the ICTY overall control standard, there is also precedent within the ICJ context itself to support a third more flexible standard of State responsibility. Specifically, the ICJ held in the *Iran hostage case* that the actions of a State's citizens could be attributed to the government if the citizens "acted on behalf on [sic] the State, having been charged by some competent organ of the Iranian State to carry out a specific operation" (United States v. Iran, 1980, p. 29). There, while the Court did not find enough evidence to attribute the actions of the citizens to the government, the Court did find that the Iranian government was nonetheless responsible because it was aware of its obligations under the 1961 Vienna Convention on Diplomatic Relations and the 1963 Convention on Consular Relations to protect the U.S. embassy and its staff, and failed to comply with its obligations (Barkham, 2001, p. 98).[3] This reasoning could be extended to cyber attacks in two ways. First, the standard could be adopted that, if the citizens of a State acted on behalf of a competent government organ, then the government could be vicariously liable for the resulting damage from such cyber attacks. Second, if there is insufficient evidence to find attribution outright, as there was in *Iran hostage*, then the standard could become one of governmental awareness, i.e. if the government was aware of its obligations under international law to prevent its citizens and information infrastructure from launching cyber attacks and failed to comply with these responsibilities. That State could then be held in breach of international law. Either the *Tadic* or *Iran hostage* standards has the benefit of moving beyond the rigid effective control framework, and holding State sponsors

3 The *Corfu Channel* case should also be considered in this context. In that case, Albania mined the Corfu Strait, and the British Royal Navy sued for damages and loss of life that it sustained as a result of ships colliding with the mines. There, the ICJ stated: "…it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein." (United Kingdom v. Albania, 1949, p. 30). Yet, even in *Corfu Channel* the Court noted that the standard of State responsibility should be somewhat flexible when it stated, "…the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility. Such a State should be allowed a more liberal recourse to inferences of fact and circumstantial evidence." (United Kingdom v. Albania, 1949, p. 30).

of cyber attacks accountable when significant evidence exists of their involvement.

Yet there are difficulties posed by adopting a standard of State responsibility with a lower burden of proof than effective control that should be addressed. Principal among these is the danger of prosecuting accused State sponsors of attacks that are in fact innocent. Politically, this worry may cause some countries to push for the higher burden of proof enshrined in the effective control standard so as not to be wrongly accused of sponsorship. Such critiques may in part be addressed though by a clarification that a requirement of 'beyond a reasonable doubt' under the overall controls standard is still a very high burden of proof that the prosecuting entity must meet, making frivolous or unwarranted cases unlikely (Erikkson, 2004, p. 294). Other outstanding issues that demand attention include the necessity of defining the appropriate forum in which to bring a case against State sponsors of cyber attacks, with candidates ranging from the ICJ, to national courts, or specialized tribunals.

In summary, it is far too easy for governments to hide their information warfare operations under the effective control standard. It should thus be sufficient as matter of international law to prove overall control by a government in a cyber attack, rather than complete control. For example, if the overall control standard were used instead of effective control, it would be possible that Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, if proven, would be sufficient to satisfy State attribution. A comprehensive future legal regime could grant Estonia, and other victim nations, adequate reparations for such attacks. But if effective control becomes the dominant paradigm for determining State responsibility for cyber attacks, even a victim State of a worst-case scenario cyber attack may not receive justice. Alternatively, the ICJ precedent of *Iran hostage* could be used as another vehicle to hold State sponsors of cyber attacks accountable. But why is this distinction critical within the context of NATO's cyber security strategy?

4. CYBER CONFLICTS AND NATO

During the 2007 cyber attack on Estonia, several Estonian officials raised the issue of whether Article 5 of the North Atlantic Treaty Organization (NATO) could be invoked, which maintains that an assault on one allied country obligates the alliance to attack the aggressor (*North Atlantic Treaty*, 1949 art. 5). This was the first time in NATO history that a member State had formally requested emergency assistance in the defense of its digital assets (Hughes, 2009). Estonia did receive the limited help that it requested from NATO. Further assistance was unavailable since NATO and the international community alike viewed the 2007 cyber attacks on Estonia as an instance of cyber crime, or cyber terrorism (Koms & Kastenberg, 2008-09, p. 63).

This was also the case in the cyber attacks against Georgia, in which there was also no conclusive evidence that Russia was indeed behind the attacks (Schapp, 2009, p. 121). This was for two primary reasons. First, the attacks were not serious enough to constitute an armed attack thus activating NATO Article 5. Second, State responsibility for the attacks could not be conclusively proven. NATO has taken steps to address the gaps in cyber security strategy that the cyber attacks on Estonia underscored, such as by creating the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, and the new Cyber Defense Management Authority in Brussels, which is a NATO effort to centralize cyber defense capabilities ("NATO opens new centre of excellence on cyber defence," 2008). But without a legal regime for State responsibility in place going forwards, such efforts are by themselves insufficient.

It is critical for NATO's future efforts in cyber security for its member States to have a comprehensive and settled standard to gauge State responsibility for cyber attacks. Specialists at the CDMA, or at the various CERTs of the member States, will not be able to gather the necessary intelligence to prove which nation or group launched a given cyber attack if the standard of proof itself is left undefined. If the effective control standard is indeed accepted as the required standard for State responsibility, then information gathering would have to be total, necessitating new technologies capable of tracking individual packets conclusively back to their true source. Alternatively, if the overall control standard is adopted by the international community, then significant evidence beyond a reasonable doubt of State sponsorship or support for cyber attacks would be sufficient to hold accountable those States, or groups within those States, that launch cyber attacks against NATO member nations or businesses operating within member States.[4] Thus, it is in NATO's own best interests to have a standard of State responsibility for cyber attacks defined, and to push for the adoption of the overall control standard over the effective control standard.

5. CONCLUSION

The domestic and global implications of human society's increasingly critical dependence on the Internet makes necessary the ability to deter, detect, and minimize the effects of cyber attacks (Lipson, 2002, p. 3). Today, NATO and the United States alike are at the point of determining how the governance of cyberspace should develop, including influencing the vector of the *jus ad bellum* from the very inception of the legal framework for cyberwarfare. The strategies and practices that are assumed in the short-term thus will greatly impact how this fast evolving body of law is shaped (Schmitt, 2003, p. 415). The case has been made in this Article that there

4 A recent well-publicized example of such a case was the cyber attack on Google in which there were questions over Chinese-government sponsorship (Shiels, 2010).

are currently two vying regimes for State responsibility under international law: the effective and overall control standards. Due to the technical difficulties with proving attribution for cyber attacks, along with the unreasonably high standards of proof imposed by the effective control standard, I have argued for the adoption of the overall control standard. This has the benefit of holding State sponsors of cyber attacks accountable where there exists sufficient proof beyond a *reasonable* doubt, as opposed to beyond *any* doubt. Adopting the overall control standard for cyber attacks is thus both within the best interests of NATO and the international community. But determining a standard for State responsibility is only one part of promoting cyber security. There are a myriad of other related issues that deserve further research and attention by scholars and policymakers alike, such as determining the appropriate forum in which to prosecute State sponsors of cyber attacks.

REFERENCES

- Barkham, J., 2001. Information Warfare and International Law on the Use of Force. *New York University Journal of International Law and Policy,* 34, 57-114.
- Brenner, S. W., & Crescenzi, A. C. 2006. State-Sponsored Crime: The Futility of the Economic Espionage Act, *Houston Journal of International Law, 28, 389-464.*
- Burgess, D. R., 2006. Hostis Humani Generi: Piracy, Terrorism and a New International Law, *University of Miami International and Comparative Law Review, 13, 293-312.*
- Capaldo, G. Z. 2007. Providing a Right of Self-Defense Against Large Scale Attacks by Irregular Forces: The Israeli-Hezbollah Conflict, *Harvard International Law Journal Online, 48, 101-112.*
- Cassese, A. 2007. The *Nicaragua* and *Tadic* Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, *European Journal of International Law, 184, 649-668.*
- Cordesman, J. 2002. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection*. Westport: Praeger Publishers.
- Davis, J. 2007, August 21, Hackers Take Down the Most Wired Country in Europe. *Wired Magazine*, p. 9.
- Erikkson, S. 2004. Humiliating and Degrading Treatment under International Humanitarian Law: Criminal Accountability, State Responsibility, and Cultural Considerations, *Air Force Law Review, 55, 269-311.*
- Gray, C. 2000. *International Law and the Use of Force*. Oxford: Oxford University Press.
- Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18, 1907, 36 Stat. 2259, 2271, T.S. 598 1907, *entered into force* 26 Jan. 1910, art. 1.
- Hanseman, R. G. 1997. The Realities and Legalities of Inform The Realities and Legalities of Information Warfare, *United States Air Force Law Review, 42, 173-200.*
- Held, D. 2006. *Models of Democracy.* Cambridge: Polity Press.
- Hughes, R. B. 2009, April, NATO and Cyber Defence: Mission Accomplished?. *NATO-OTAN.*
- Hunter, D. 2003, Cyberspace as Place and the Tragedy of the Digital Anticommons, *California Law Review, 91, 439-514.*
- "Internet: General Usage Statistics," http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/internet.htm.
- Janczewski, L. & Colarik, A. M. 2008. *Cyber Warfare and Cyber Terrorism*, Cambridge: CUP, 2008.
- Johnson, D. & Post, D., 1996, Law and Borders – The Rise of Law in Cyberspace, *Stanford Law Review, 48, 1367-1402.*
- Joyner, C. C. & Rothbaum, W. P., 1993, Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?, *Michigan Journal of International Law, 14, 220-260.*
- Koms, S. W. & Kastenberg, J. E., 2008, Georgia's Cyber Left Hook, *Parameteres—U.S. Army War College Quarterly, 38, 60-76.*
- Lessig, L. 1999, The Law of the Horse: What Cyberspace Might Teach, *Harvard Law Review, 113, 501-549.*
- Lipson, H. F. 2002, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, *CERT Coordination Center.*
- Luban, D. 2007, February 15, Timid Justice: The ICJ should have been harder on Serbia, *Slate.*
- Lulasik, S. 2003. *Protecting Critical Infrastructures Against Cyber-Attack*. Oxford: Oxford University Press.
- Markoff, J. & Kramer, A. E. 2009, December 12, In Shift, U.S. Talks to Russia on Internet Security, *New York Times.*

- Military and Paramilitary Activities Nicar. v. U.S. 1986 I.C.J. Rep. 14 Jun. 27.
- NATO 2008, May 20, NATO opens new centre of excellence on cyber defence, *NATO News.*
- North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241U.N.T.S. 243.
- Pronk, R. J.P. 1997, ICTY Issues Final Judgment Against Dusan Tadic in First International War Crimes Tribunal Since World War II, *Human Rights Brief, Center for Human Rights and Humanitarian Law.*
- Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 Oct. 2, 1995.
- Reich, R. B. 1991. *The Work of Nations: Preparing Ourselves for 21st-Century Capitalism.* New York: Vinage Press.
- Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/56/10 Dec. 12, 2001.
- Russian-Estonian MLAT.
- Ryan, J. 2007. *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web.* Dublin: IIEA.
- Schmitt, M. N. 2003, The Sixteenth Waldemar A. Solf Lecture in International Law, *Military Law Review, 176, 364-421.*
- Schmitt, M. N. 1998, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law, 7, 885-937.*
- Schapp, A. J. 2009, Cyberlaw Edition: Cyber Warfare Operations, Development and Use Under International Law, *Air Force Law Review, 64, 121-173.*
- Shackelford, S. J. 2010, Estonia Three Years Later: A Progress Report on Combating Cyber Attacks, *Journal of Internet Law, 138, 22-29.*
- Shackelford, S. J. 2009, From Net War to Nuclear War: Analogizing Cyber Attacks in International Law, *Berkeley Journal of International Law, 25, 191-250.*
- Shackelford, S. J. 2007, Holding States Accountable for the Ultimate Human Rights Abuse: A Review of the ICJ Bosnian Genocide Decision, *Human Rights Brief, 14, 21-26.*
- Shiels, M. 2010, 14 January, Security Experts say Google Cyber-Attack was Routine, *BBC News.*
- The Application of the Genocide Convention Case Bosnia and Herzegovina v. Serbia and Montenegro, 2007 I.C.J. 140 Feb. 26.
- The Corfu Channel Case United Kingdom-Albania, 1949 I.C.J. 4ff.
- Tosh, C. 2007, March 2, Genocide Acquittal Provokes Legal Debate, *Institute for War and Peace Reporting.*
- United States Diplomatic and Consular Staff in Tehran U.S. v. Iran, 1980 I.C.J. 3, 29 May 24.
- U.S. Department of State 2007, *Treaties in Force* http://www.state.gov/s/l/treaty/treaties/2007/index.htm
- Verton, D. 2003. *Black Ice: The Invisible Threat of Cyberterrorism.* Cambridge: CUP.
- Watkin, K. 2004, Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict, *American Journal of International Law, 98, 1-34.*
- White House 2003. *National Strategy to Secure Cyberspace,* 19.
- Wolf, J. B. 2000, War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money, *American Criminal Law Review, 28, 95-117.*
- Yang, D. W. 2006, Countering the Cyber-Crime Threat, *American Criminal Law Review, 43, 201-215.*

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

THE CYBER THREAT TO NATIONAL SECURITY: WHY CAN'T WE AGREE?

Forrest HARE[a,1]

[a]*School of Public Policy, George Mason University*

Abstract: In March 2009, the Organization for Security and Cooperation met for its first workshop on cyber security. Though the discussion was insightful, the representatives to this workshop could not reach unanimous agreement regarding the important cyber security issues on which the forum should focus. For example, some representatives believed there is a looming arms race that must be countered while others were most concerned about mounting cyber crime. As the threat from a multitude of actors in cyberspace increases, why is it difficult to reach consensus on the most pressing threats to national security? This paper postulates that different national agendas and different technology levels amongst the world's nations will lead to different prioritization of the cyber security threat. Using the Barry Buzan vulnerabilities framework, this paper will explore how countries may be driven to prioritize potential cyber threats differently. This paper concludes that, unless these national differences are accounted for, concerted international efforts to improve inter-country cooperation will be met with confusion, at best, and resistance, at worst, on the part of national, international, and private sector stakeholders.

Keywords: cyber security, security studies, neorealism, security alliances

1 Corresponding Author: Forrest Hare; E-mail: fhare@gmu.edu.

INTRODUCTION

"…the term 'security' covers a range of goals so wide that highly divergent policies can be interpreted as policies of security."

Arnold Wolfers (1952)

In March 2009, government experts from the Organization for Security and Cooperation (OSCE) met in Vienna for the organization's first workshop on cyber security. Though the discussion was insightful, the representatives to this workshop could not reach unanimous agreement regarding the important cyber security issues on which the forum should focus. For example, some states arrived with the message that there is a looming cyber arms race that must be countered (Streltsov, 2007); but official statements suggest that most attendees were primarily concerned about mounting cyber crime and collaborating on security measures (Vershbow, 2009). The debate over cyber security priorities is not limited to the OSCE. Nor is there agreement that cyber security threats constitute significant risks to national security. Some influential researchers providing analyses for their governments downplay the significance of many of the alarming cyber scenarios to national security (see, for example, Libicki, 2009; Cavelty, 2007). In spite of this, the United States has publicly stated in a recent cyber policy review that existing vulnerabilities in cyberspace "have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests (Obama, 2009)." So if most advanced and advancing nations consider cyber security important to their nation, why is it difficult to reach consensus on the most pressing threats in cyberspace to national security? In this paper, I argue that differing endowments of national power and socio-political cohesion amongst the world's states will lead them to characterize and prioritize cyber security threats differently. The divergent perspectives that result will impede any efforts to reach consensus on actions to counter existing cyber threats. An important first step to gaining consensus is understanding these perspectives.

The paper will begin with a discussion of the place of cyber security in the larger debate of security issues. It is important to begin placing cyber security in the context of national security matters since the issues are most often relegated to technology debates. In this section I will argue that cyber threats can be viewed as national security matters and therefore should be relevant to the security studies field and should be analyzed using security studies theories. The section concludes with a presentation of the Buzan framework for categorizing vulnerabilities taken from his book, *People, States, and Fear (1991)*. The Buzan framework classifies several potential threats to national security as viewed by different types of states. In the section that follows, I will attempt to extend the Buzan model to cyber security issues. The

categorization will be illustrated with recent examples of statements by national leaders and organizations. Lastly, I will address several implications these divergent national viewpoints have on policy formulation.

1. CYBER SECURITY AS NATIONAL SECURITY

In this section, I will place cyber security in the greater field of security studies. To do so, requires an assessment of the securitization process and how cyber threats have been securitized by a diverse set of stakeholders. The goal of this section is to demonstrate that cyber threats may be considered national security issues and therefore, theories from the security studies field, specifically the Buzan vulnerabilities and threats framework, can be applicable to cyber security research and policy.

In his seminal article, '"National Security" as an Ambiguous Symbol', Arnold Wolfers (1952) asserts that the decision to classify a threat as being one to national security, and the measures that will be taken, are political decisions, not technological or legal. Buzan et al (1997), writing half a century later, delved more deeply into the process of moving a political agenda into the forefront of security – process they call, "securitization." In other words, when an issue is presented as posing an existential threat (usually to the entire nation-state) such that it requires emergency measures (those that go beyond normal political actions), then it is being securitized (Buzan et al, 1997). Therefore, a threat, victim, and understanding of the threat to the victim, are all required to engage in the process. In cyberspace, the threat agents can be criminals, hackers, terrorists, and nation-states. The potential victims at risk from these threat vectors are also diverse. The threat actors may be in the business of stealing personal identities to commit fraud that, in the inter-connected world of cyberspace, would make all individuals in a nation potential victims. Or the threat actors may be conducting industrial espionage. In the case espionage, the direct victims are the target companies, but if the stolen information is the plans for a new fighter aircraft, the taxpayer may again be considered a victim. In cases where the identified victim is the state and its institutions, the existential threat may be one of toppling the regime or one from break-away sections of the country. In cases where individual citizens face an existential risk to their welfare, either directly or through a loss of state institutions, a justification for public action can be made because national defense is considered a public good. Politicians are therefore motivated to securitize threats to individual citizens because they are charged to represent their constituents' interests.[2] Ultimately, several potential threats to many differ-

2 And, of course, the politician will lose their office if they don't represent their constituents' interests.

ent stakeholders can exist in cyberspace. One can appreciate that broad arrays of threat actors, and broader consideration of potential victims can lead to a variety of securitization attempts.

The ambiguous nature of national security in cyberspace also contributes to the debate about the scope of national security within the academic field of security studies. On one end of the security studies spectrum sits the neorealists. The neorealist view is championed by Stephen Walt of the Kennedy School. In an effort to form clear boundaries and ostensibly foster objective analysis, Walt (1991) contends that security studies should focus on the "phenomenon of war" as conducted by military powers under the political control of state actors. He would also include other issues of statecraft directly related to military affairs, such as arms control and crisis management, because they influence the potential for and character of war (Walt, 1991). Most likely, neorealists would argue against expanding the security studies agenda to include cyber security as long as there is still debate about the true impacts of cyber attacks to a nation's physical security, and to its military capability (for discussions of this debate, see Cavelty, 2007; Kelly & Fitzgerald, 2009; Libicki, 2009).

Researchers associated with the Danish Peace Research Institute, such as Barry Buzan, and Ole Waever, occupy the other end of the spectrum from the neorealists. Their view of security studies accepts a much broader, and deeper agenda. For example, they recognize security threats as emanating from military and political actors, but they also highlight the potential for economic, societal, and ecological threats to national security (Buzan, 1991). In addition, the referent object being threatened can encompass any actor from the individual to international level, including such actors as corporations, nations, states, and communities (Buzan et al, 1997). In this sense, cyber threats would clearly constitute security issues for a referent object even if the actor is an individual and the existential threat is a threat of economic ruin.[3]

The neo-realists and other security studies experts would not agree on the place of cyber security in the field, it is clear that states have decided there is a cyber security component to national security. As long as representatives of nation-states continue to securitize cyber threats in speeches and proposals, we must consider the role that these issues play in national security, and many academics in the field would agree. As Krause and Williams (1996) argued in their attempt to reconcile the competing academic view points, even if we are to focus on the emergency measures of nation-states, we must understand the "why" aspect of securitization. Often the "why" aspects of national security deal with the security views of stakeholders at the non-state level, and threats that emanate from non-state actors. This pertains to cyber security as well. As many authors have argued, nation-states do not hold the

3 Neorealists would have critiques for all these points, but space does not allow for a continuation of the exchange.

monopoly on malicious capabilities in the domain (see, for example, Kramer, Starr, & Wentz, 2009). In addition, a cyber threat has the potential to span all levels of security very quickly based on the speed with which actions can occur and based upon our inter-connectedness in the domain. In a nod to the neorealist, the states most play a central role in addressing cyber threats to national security because they remain the actors with the power, and authority, to improve defenses against most existential cyber threats. While it is true the private sector actors in most countries are critical to security in cyberspace, as Krause and Williams (1996) have stated, "there can be no security in the absence of authority (p. 232)."

Having argued that cyber threats can be analyzed from the perspective of security studies, I will now present a framework for assessing the different perspectives on cyber security vulnerabilities, based on the characteristics of the state, taken from this field. This framework was originally presented in Buzan's oft-cited book, *People, States, and Fear* (1991). To construct this framework, Buzan focuses on two key aspects of nation-states—power and socio-political cohesion. Power (or weakness) can be assessed relative to the military capabilities commanded by other states in the international system, specifically, neighbors and great powers (Buzan, 1991). Most often, weak powers must specialize their economies in order to prosper, but this specialization does not completely reduce vulnerabilities. States that do not exhibit strong socio-political cohesion are vulnerable to threats to the idea of the state, its institutions and even its territorial integrity (Buzan, 1991). Buzan recognizes the difficulty with absolute measurement of either these two factors. Therefore, this model is most effective when restricted to a comparative analysis of states relative to others in the international system. The resulting combinations of national power and socio-political cohesion, with which to assess the relative importance of threats from the perspective of the state, can be depicted in a simple matrix. Table 1 depicts the four possibilities such a model presents.

Table 1. Vulnerabilities and Types of States (taken from *People, States, and Fear* (1991))

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	Highly vulnerable to most types of threats	Particularly vulnerable to military threats
	Strong	Particularly vulnerable to political threats	Relatively invulnerable to most types of threat (less inclined to characterize issues as military)

Weak powers that also experience weak socio-political cohesion (P-W/SC-W) will obviously be the most vulnerable to all threats to their security at all levels and from all sectors. When such states contain resources that are of value to others, they are mostly likely under constant threat that will further exacerbate their developmental challenges (Buzan, 1991). Equally straightforward is the situation confronted by strong powers that are also socio-politically cohesive (P-S/SC-S). According to the Buzan model, such states have far fewer vulnerabilities, making it more difficult for stakeholders to successfully securitize their security agendas. In other words, even stakeholders in P-S/SC-S states will attempt to securitize issues for a host of reasons; however, the action is only successful if the collective state accepts the implementation of emergency, extra-political, or extra-legal, measures to respond to the threat (Buzan et al, 1997). In such a state, the regime faces more resistance to such measures from the populace.

States along the opposite diagonal, bottom left to top right, may have greatly divergent views of security threats. The bottom left category demonstrates the priority of states that have relatively strong militaries, but relatively less socio-political cohesion (P-S/SC-W). According to this model, these states are most concerned about the threats posed to the state's ability to maintain control over the populace. As Buzan (1991) states it:

> *"Weak states, and those with narrowly cast ideological orthodoxies, will be impelled by their domestic conditions to push the qualifications for threats to have 'national security problem' status down towards the low end of the threat spectrum. When political threats dominate, the national security agenda can become very wide-ranging indeed (p. 115)."*

Such a condition can easily lead to the continuous imposition of emergency measures and authoritarian regimes.

States in the top right quadrant have a fundamentally different perspective of their vulnerabilities to national security threats. According to the model, these states are characterized by their inability to generate significant military power but they have established strong socio-political cohesion within their borders (P-W/SC-S). Examples of such states might be small European countries and the Tigers of Asia. Since these states have stable, robust institutions, they are much less concerned about political and ideological threats to their existence. However, P-W/SC-S states are acutely vulnerable to their neighbors' military power. Limited resources may force such states to specialize economically, but this specialization makes their security situation no less fragile.

Obviously, this framework is not designed to comprehensively classify all types of states, nor depict all the potential threats against which a state will consider itself

vulnerable. As stated earlier, all analyses of state behavior within the international system can only be assessed relative to other states. However, the model's coarse classification allows the researcher and policymaker to understand the intersections of two polemics, regarding power and socio-politics, and how these characteristics potentially influence the security agendas of many states. This framework provides a compelling starting point when assessing the securitization actions of states both internally and in international forums. Perspectives and prioritization of security threats vary most markedly from the bottom left quadrant to the top right. In addition, states in the bottom right and top left quadrants may share perspectives of states in the top left and bottom right quadrants depending on the nature of the threat, and their relative vulnerabilities to the threat, at any given time. For example, a P-S/SC-W state may find support from P-W/SC-W states for justifying measures to combat ideological threats if both are sensitive of a minority's separatist agenda, even if the states do not have common ideologies or the same minority. In international engagements, P-W/SC-S states may find support for the relative prioritization of certain threats against critical infrastructure, if not the magnitude of the threat, from P-S/SC-S states. Clearly, any efforts toward consensus views on security issues will be met with structural resistance. We should expect cyber security to be no different.

2. SECURITY STUDIES APPLIED TO CYBER SECURITY

As argued earlier, the potential for existential threats to states' and individuals' security can exist via cyberspace. Therefore, cyber security can be viewed from the standpoint of national security. It then follows that models used to understand national security should also be applicable to studying cyber security issues. In this section I will present a possible construct for such an application.

Whereas the Buzan framework was developed for security issues in general, Table 2 depicts potential ways that various nation-states would securitize their vulnerabilities to cyber threats.

P-W/SC-W: According to this model, states that fall into the top-left quadrant will be concerned about most all types of threats that can occur in cyberspace from destabilizing political web forums, to attacks on any Internet infrastructure, to criminal actions that can quickly undermine their financial systems and citizens' welfare. The government institutions in such states most likely lack expertise both on how to secure their IT systems, but also to understand the true extent of the threats the face. Some threats may be much more substantial than government officials may anticipate, such as their vulnerability to e-government website hacks. Other threats,

in that they are difficult to quantify due to animosity and ambiguity, may lead to a heightened fear of the unknown. For example, a statement made by the Georgian National Security Council chief, Eka Tkeshelashvili, at 2009 GovSec Conference characterized computer scientists in a foreign nation as "soldiers" who worked with other non-governmental "mercenaries" in a concerted cyber attack on her country (Shachtman, 2009). Such statements can be analyzed to find evidence for how cyber threats are be securitized by a P-W/SC-W state.

Table 2. Cyber Vulnerabilities and Types of States

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDOS and other major attacks on critical infrastructure*
	Strong	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

* A distributed denial of service attack, or DDOS, occurs when many computers, usually surreptitiously controlled, are used to inundate a web server with requests and cause it to become overwhelmed to the point that service is denied.

P-S/SC-S: Moving on the diagonal from the top left to bottom right quadrant, P-S/SC-S states have the ability to maintain stronger military and economic forces within the international system, and are therefore most reluctant to securitize threats in cyberspace at the same level they have for more conventional threats. Because they recognize that would-be adversaries can potentially hold their critical infrastructure at risk in cyberspace, there has been substantial writing on this potentiality in many technologically advanced countries (see, for example Kramer et al, 2009; Cavelty, 2007; Arquilla & Ronfeldt, 1998). Absent a significant attack, the true extent of vulnerability is difficult to measure. As a result, few states have effectively securitized these vulnerabilities to the degree they have securitized conventional military and terrorist threats. For example, no states in this category have begun to heavily regulate cyber security in critical infrastructure sectors (Assaf, 2008; Brown, 2006). In these states, cyber security typically remains a responsibility of the private sector owner-operators.

As discussed earlier, P-S/SC-S states are technologically advanced relative to those in the top left quadrant. They also have larger economies and therefore rely heavily on cyberspace for financial transaction and the development of intellectual prop-

erty. Because the value of information and finances that are stolen in cyberspace can be directly measured, stakeholders in these economic sectors may have more success securitizing their vulnerabilities. For example, though it did not explicitly list crime as the most significant cyber threat, the cyberspace policy review (2009) conducted by the Obama administration stressed at several points the need to improve international cooperation on information and finance protection issues. It states, " the United States should accelerate efforts to help other countries build legal frameworks and capacity to fight cyber crime and continue efforts to promote cyber security practices and standards (p. 33)." In addition, none of the recommendations in the report support the enactment of emergency, extra-political measures to improve national security.

P-W/SC-S: In a conventional sense, P-W/SC-S states are vulnerable to most threats of military force because their infrastructure and population are highly-susceptible to military attacks. Small countries that have strong socio-political cohesion are often highly developed countries that have made the full transition to e-governance. Citizens may now be dependent on cyberspace for every day life. As these countries have advanced technologically, their infrastructure has become inter-linked and inter-dependent through this medium. This advancement has made such systems equally vulnerable to cyber attacks. However, such countries may find it difficult, either physically or financially, to develop the redundant capabilities and bandwidth that would be required to withstand concerted attacks on their cyber infrastructure. Such states would therefore be most inclined to securitize the threat of DDOS and other major cyber attacks on critical infrastructure. As a result, P-W/SC-S states are most interested in developing strong security measures that will make their infrastructure systems less vulnerable to cyber attacks, as well as supporting international efforts that will categorize cyber attacks on their infrastructure as threatening as physical attacks. A recent strategy report by the Estonian Ministry of Defence contains statements that could be used as evidence for this focus of securitization. For example, the top cyber threat identified in this strategy is attacks against critical infrastructure (Estonia, 2008). The only other threat this report identifies is the threat of cyber crimes committed for financial gain.

P-S/SC-W: As stated earlier, countries that are militarily powerful, yet lack strong social-cultural cohesion within their borders, tend to securitize the threat of de-stabilizing rhetoric emanating from within its borders, and from hostile parties abroad. Cyberspace has now vastly increased the challenge for central regimes that desire to control the spread of information they consider subversive. For one, it allows greater anonymity to those who would publish the rhetoric. Second, the spread of cyberspace allows for much quicker communications. And third, it links communities both within and outside of a country. This increased linkage facilitates alternative interpretations of internal events for the international community. Because

the tools of messaging are open to all, the bar is raised for P-S/SC-W. Such states see the spread of cyberspace and the influence of the Internet as de-stabilizing to their efforts to improve social-cultural cohesion and maintain existing state institutions. Accordingly, these countries would be most interested in enacting measures that will justify greater control of information flowing through cyberspace, both within their sovereign territories and to the international community. An article by Streltsov (2007), a member of the Russian delegation to the UN Group of Governmental Experts to a cyber security meeting in 2004, contains extensive language regarding his country's concern for socially de-stabilizing actions in cyberspace. For example, he identifies threats that "undermine a state's economic and social systems and psychological manipulation of a population for the purpose of destabilizing society (p. 8)," as ones that require international efforts to combat. In fact, his government stresses the concept of "information security" above "cyber security." According to Streltsov (2007), the idea of information security concerns threats such as; "spreading disinformation or creating a virtual picture partially or totally misrepresenting reality in the communications sphere; or producing disorientation, loss of will power or temporary destabilization among the population (p. 7)." These are clearly threats of a political nature that would conform to the Buzan model as being representative of a P-S/SC-W state's desire to maintain internal cohesion.

As with conventional threats, states in different quadrants may form cyber "securitization alliances." For example, the Estonian cyber security strategy highlights many of the same threats that the US cyber policy review identified. It is possible that these two nations, when discussing issues in international forums, may support each other's efforts to securitize specific threats such as cyber crime. Also as with conventional threats, perspectives and prioritization of security threats would be expected to be most divergent from the bottom left quadrant to the top right. According to this model, P-W/SC-S states would not prioritize the threat from the spreading of disinformation as highly as a P-S/SC-W state relative to the threat from attacks on critical infrastructure. Therefore, one would expect little, if any, agreement between states in these two quadrants during international forums on cyber security issues regardless the unique relationships between the states.

The discussion above might suggest that I have categorized specific countries according to this model. On the contrary, I will not do so in this paper for two reasons. First, the statements used as example evidence were merely intended to show representative acts of stakeholders securitizing particular cyber threats. Though they were from official sources, they were not meant to suggest that the states these actors represent are necessarily representative of a specific quadrant, nor that the cyber threat highlighted in the statement is always the most important one from their state's perspective. This is not to say that future research could not gather empirical evidence to conduct such an analysis. Secondly, the dynamic nature of

cyberspace makes it probable that countries will find themselves shifting between the quadrants in the matrix. For example, a country that is normally considered to be socio-culturally cohesive may abruptly find its state in a weak position because a de-stabilizing influence on the Internet, such as a video of police attacking students, spreads quickly through cyberspace. Or, a country that is normally considered to have weak socio-cultural cohesion may confront a military threat that improves their cohesion, but places their cyber infrastructure directly at risk. This combination would lead to a prioritization of threats that is characteristic of the right-hand column. Any useful analysis from a public policy standpoint must account for how these dynamics influence international interactions on cyber security.

3. PUBLIC POLICY IMPLICATIONS AND CONCLUSIONS

All securitization acts are conducted to support an agenda for public or state-directed action. In this section, I will address two ways this model could support public policy formulation and analysis. First, I discuss how the framework can help policymakers understand and reconcile competing policy agendas that result from securitization of cyber threats. Then I postulate how the divergent perspective of cyber security threats from Table 2 may impact existing security alliances.

Policy analysts and policymakers are often confronted with recommendations for public action that seem to be contradictory, or at least in some way conflicting, when presented side-by-side. For example, one stakeholder may argue for a test ban to halt the development of "cyber weapons" while another may call for greater funding for cyber forensic analysis. For international organizations, such as the UN or NATO, proposals may be assessed without a complete understanding of how or why the threat leading to the proposal had been securitized. The model in this paper based on the Buzan vulnerability framework, can support cyber security policy formulation and coordination in at least two ways. First, using the model to assess the underlying assumptions and overall security agenda of relevant state actors can add needed perspective to an analysis of competing cyber security proposals. In addition, a wider acknowledgment and understanding of the assumptions behind the cyber security agendas of state actors and other stakeholders may reduce the potential for security or defense dilemmas in the cyberspace.

Ultimately, nation-states have two options to reduce their insecurity; they can either make themselves less vulnerable to security threats, or attempt to prevent or lessen perceived and real threats (Sundelius, 1983). There is no clear principle that supports efficacy of one policy direction over another. Even if all stakeholders agree that a threat should be securitized, it does not guarantee agreement on the correct

response to the threat. Strong arguments can be made for taking either, or both routes. Wolfers (1952) provided a useful illustration. If one nation had a policy to maximize its security by relying on armaments and alliances, while another did so based on maintaining strict neutrality, "a policymaker would be at a loss where to turn (Wolfers, 1952, p. 490)." In cyberspace, there are many proposed solutions to addressing a wide array of threats. For example, Libicki (2009) concludes in his recent monograph, Cyberdeterrence and Cyberwar, that the best way for the US military to improve cyber security is by improving computer security measures. This solution may be likened to the position of maintaining strict neutrality. Streltsov (2007) argues that the international community should forbid the use of information and communications technologies that are used to damage critical infrastructure. This solution is akin to arms control policies and treaties. Finally, a 2008 study to prepare the new US president to address cyber security challenges recommended strong federal oversight of both governmental and private actions (while being careful to highlight civil liberty issues) (Lewis, 2008). These, and other policy agendas by state and non-state stakeholders are all based on securitization of particular cyber threats. Disagreement of the feasibility of these recommendations is compounded by disagreement on the significance of underlying threats. As stated above, important first step toward consensus on policy measures is to understand and try to rectify the disagreements on the securitization acts behind the policy proposals. The framework presented in this paper is a tool that can be used to assess the underlying cyber threats and how each stakeholder sees them as being significant. For example, Libicki's proposal to rely on network security to combat cyber threats is a practical proposal if the object of interest, in this case, the US military, is not vulnerable to political threats. According to the framework, this proposal would probably not meet with widespread acceptance in international forums where other participants consider political threats in cyberspace to be significant. Policymakers must recognize these influences before expending unnecessary diplomatic energy on their policy agendas.

Another concern that stems from differing perspectives on the significance of cyber threats is the potential for a security dilemma in cyberspace (Hare, 2009). As characterized by Herz (1950), a security dilemma may arise as one nation's efforts to arm themselves in defense may provoke another nation to do likewise, thereby creating a greater threat. Since it is much more difficult to make public or confirm the defensive nature of cyber security measures, other states may characterize any actions as potentially hostile. Differing perspectives on the significance of cyber threats will compound these misperceptions. For example, investments in technologies to secure e-governance sites and information forums may not be seen as threatening by states that do not consider themselves vulnerable to political threats. However, P-S/SC-W states may interpret these measures as preparations for information attack purposes and therefore feel threatened by them. For this reason, it is important for

one state to be aware of differing perspectives on cyber security in order to understand how other states will perceive their cyber security measures.

The existence of differing perspectives of cyber security based on the framework presented in this paper may have interesting, yet counter-intuitive implications for cyber defenses within a security alliance. In their analysis of the NATO security alliance from an economic perspective, Olson and Zeckhauser (1966) addressed the traditional complaint that larger countries bear a disproportionate burden of providing for the alliance's defense. Collective action theory suggests that larger nation's place a greater value on the alliance while smaller nations tend to free-ride. In their study, the authors discover that when there is a decline in the strength of the alliance, expenditure on defense goes up amongst the smaller nations. The result is that, as long as the alliance holds, the overall expenditure may come closer to the optimal level (Olson & Zeckhauser, 1966). This observation has implications for cyber security within a security alliance as well. If the member nations of the alliance have different perspectives on cyber security based on Table 2, they will have difficulty agreeing on how the alliance should work together to defend against cyber threats. Some states will assert that they must work together in the areas of law enforcement and not consider military response actions to cyber attacks. Others may lobby for collective military responses if they consider threats to their infrastructure to be existential. In the absence of concurrence, each member state will be required to create their own strong cyber defenses against all potential threats they consider existential. Therefore, as long as the alliance generally holds in the face of a concerted attack across the alliance, the lower level of cohesion may actually improve the defensive response. Due to the inter-connectedness of states and reduced relevance of geography in cyberspace, on state cannot provide a security umbrella for the entire alliance. In fact, one should assume that all states are equally at risk in cyberspace and therefore require their own defenses of their critical cyber systems. At the same time, an unsuccessful defense in any one nation may have a significant impact on the entire alliance. As a result, it is possible this counter-intuitive outcome of differing security agendas may improve the defenses of all nations in the alliance.

In this paper, I have argued that threats in cyberspace can be viewed as concerns for national security. However, as with all issues of national security, multiple perspectives must be expected. This paper introduced a framework, based on work by Barry Buzan of the Copenhagen School of Security Studies, with which to assess divergent and complimentary perspectives of vulnerability to threats in cyberspace. This framework incorporates a consideration of both military power and socio-political cohesion in order to understand what threats may be considered threats to national security. While the model was not tested empirically, it does suggest that states in each quadrant of the matrix may not support policy agendas of states in other quadrants with divergent perceptions of their vulnerabilities in the domain.

As with all collective action at the international level, a coalition of diverse actors must be built in order to make progress toward the collective good. Therefore, the model can be useful to identify areas of consensus between different states. The coalition may begin with a small "securitization alliance" and then expand to include others that are not completely aligned, but can find common ground in an effort to achieve a measure of progress. Once states in three of the four quadrants have joined in the coalition, they may encourage commitment from actors with the most divergent viewpoint. For example, this may be one strategy to bring the P-S/SC-W and P-W/SC-S states together on a security agenda they would otherwise not desire to support. But as long as states within the international system occupy all four quadrants, any international efforts toward greater security in cyberspace must contend with divergent security agendas based on differing prioritization of the multitude of threats in the medium.

REFERENCES

- Arquilla, J., & Ronfeldt, D., 1998. Cyberwar is Coming! In G. Stocker & C. Schoepfer (Eds.), *Infowar* (pp. 24-50). New York: Springer Verlag.
- Assaf, D., 2008. Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection, 1,* 6-14. doi:10.1016/j.ijcip.2008.08.004
- Brown, K., 2006. *Critical Path.* Fairfax, Virginia: Spectrum Publishing Group.
- Buzan, B., 1991. *People, states, and fear: The national security problem in international relations* (2nd ed.). Boulder: Lynne Rienner.
- Buzan, B., Wver, O., Wilde, J. D., & Waever, O., 1997. *Security: A New Framework for Analysis.* Lynne Rienner Pub.
- Cavelty, M. D., 2007. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (1st ed.). Routledge.
- Estonia., 2008. *Cyber Security Strategy* (Committee Report). Tallinn, Estonia: Ministry of Defence.
- Hare, F., 2009. Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield:Perspectives on Cyber Warfare,* Cryptology and Information Security. Tallinn, Estonia.
- Herz, J. H., 1950. Idealist Internationalism and the Security Dilemma. *World Politics, 2*(2), 157-180. doi:10.2307/2009187
- Kelly, J., & Fitzgerald, B., 2009. When a Cup of Coffee Becomes a Soy Decaf Mint Mocha Chip Frappuccino. *Small Wars Journal.* Retrieved January 31, 2010, from http://smallwarsjournal.com/blog/2009/09/when-a-cup-of-coffee-becomes-a/
- Kramer, F. D., Starr, S. H., & Wentz, L., 2009. *Cyberpower and National Security* (1st ed.). Potomac Books Inc.
- Krause, K., & Williams, M. C., 1996. Broadening the Agenda of Security Studies: Politics and Methods. *Mershon International Studies Review,* 40(2), 229-254.
- Lewis, J., 2008. *Securing Cyberspace for the 44th Presidency* (Commission Findings) (p. 72). Washington, D.C.: Center for Strategic and International Studies. Retrieved from http://www.csis.org/index.php?option=com_csis_pubs&task=view&id=5157
- Libicki, M. C., 2009. *Cyberdeterrence and Cyberwar.* RAND Corporation.
- Obama, B., 2009. Cyberspace Policy Review. Executive Office of the President. Retrieved from http://www.whitehouse.gov/cyberreview/documents
- Olson, M., & Zeckhauser, R., 1966. An Economic Theory of Alliances. *The Review of Economics and Statistics, 48*(3), 266-279.
- Shachtman, N., 2009). Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It. *Wired.* Retrieved from http://www.wired.com/dangerroom/2009/03/georgia-blames/
- Streltsov, A., 2007. International information security. *Disarmament Forum, 3,* 5-14.
- Sundelius, B., 1983. Coping with structural security threats. In O. Hoell (Ed.), *Small States in Europe and Dependence.* Wien: Austrian Institute for International Affairs.
- Vershbow, A., 2009. *OSCE: Building a Europe Whole, Free and at Peace.* Washington, D.C. Retrieved from http://www.csce.gov/index.cfm?Fuseaction=Files.Download&FileStore_id=1531
- Walt, S. M., 1991. The Renaissance of Security Studies. *International Studies Quarterly, 35*(2), 211-239.
- Wolfers, A., 1952. "National Security" as an Ambiguous Symbol. *Political Science Quarterly, 67*(4), 481-502.

Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

UNDERSTANDING CYBER OPERATIONS IN A CANADIAN STRATEGIC CONTEXT: MORE THAN C4ISR, MORE THAN CNO

Melanie BERNIER and Joanne TREURNIET

Defence Research and Development Canada[1], Ottawa, Canada

Abstract: In the Canadian Forces (CF), cyber operations are currently considered to be primarily computer network operations (CNO), where CNO is categorized as a subset of C4ISR, providing support to operations in the physical environments. We contend that to use these capabilities to their fullest extent, an integrated operational environment is required, and that the current CNO model, comprised of three separate activities (computer network attack, computer network defence and computer network exploitation), must be abandoned in favour of an integrated model of cyber operations. In fact, cyber operations can be any combination of these activities and more, even drawing support from operations in other environments. To justify the cyber environment as its own battle space, we analyse cyber operations in terms of the CF's six functional domains: Command; Sense; Act; Shield; Sustain; and Generate. We discuss the challenges brought about by two fundamental sources: first, the cyber environment is dynamic relative to the physical environments; second, the cyber environment is indistinct in terms of boundaries, be they physical, political, socio-economic, or otherwise. We conclude by arguing that cyber strategies should be developed by looking at the full spectrum of cyber operations rather than focussing solely on CNO to ensure that all cyber effects are considered.

Keywords: computer network operations, cyber operations, Canada, battle space

1 Defence R&D Canada [DRDC CORA SL 2009-055].

INTRODUCTION

The Department of National Defence (DND) in Canada has identified the need for capabilities and flexibility in addressing asymmetric threats such as cyber attacks in the "Canada First Defence Strategy" (DND, 2008). There is great debate at the strategic level within the Canadian Forces (CF) on how to address the development of cyber capabilities. Although the concept of cyberspace has been around for some time, it is only recently that operations in the cyber environment are becoming more of a reality/necessity. The CF have been conducting computer network defence activities for some time now; however, it is considered to be tactical and a support element to operations. But as Canada's allies are developing programs for cyber capability development, the CF's senior leadership recognizes that there is a cyber deficiency that needs to be addressed. The problem that they face is that this area is not well defined, i.e. there is no agreed upon definition of what the cyber environment is and what it consists of. Consequently they cannot have a good understanding of how it will affect our future force structure.

Currently, concept development in the cyber environment is occurring under the leadership of Command, Control, Communications and Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) oversight committee; specifically, under the Command functional domain which will be described in section 2. In the CF's C4ISR Capability Development Plan (DND, 2009a, Annex D, p.1), the definition of C4ISR is given:

> *Consists of the concepts, the connectivity, the information systems, the sensors, and the tools in support of and required to achieve effective Command, Control and awareness across the entire spectrum of CF operations through the timely attainment, generation and distribution of trusted and relevant information.*

While cyber operations clearly contribute to the C4ISR capability, we will argue in this paper that the concept is sufficiently distinct to merit its own development field. The intent of this paper is twofold: to provoke discussion by challenging how the CF currently sees cyber operations and to enable better understanding for decision-makers at the strategic level by presenting some possibilities in future cyber operations for the CF; and, to provoke discussion among NATO allies regarding the concept and definitions proposed herein. We will present cyber operations in terms of the CF's six functional domains: Command; Sense; Act; Shield; Sustain; and Generate. By analyzing cyber operations in this manner, we can demonstrate the complexity of cyber operations, which will contribute to the argument that the cyber environment should be recognized as its own battle space.

In Section 1, we will set the scene for discussion by providing definitions of the cyber environment and cyber operations for this paper[2]. In Section 2, we will discuss a strategic level view of cyber operations, as described above. Challenges to carrying out cyber operations will be highlighted in Section 3, and we will conclude in Section 4 with a proposal for the way ahead for the CF on the development of future cyber operations.

1. ELEMENTS OF CYBER OPERATIONS

The DND/CF has no approved definition of the cyber environment, or cyberspace. Under consideration is the US Department of Defence (DoD) definition of "a global domain[3] within the information environment consisting of interdependent network information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers" (DoD, 2009, p. 139). This definition, however, does not implicitly take into account the software and information that reside on the network: these are potential targets of a cyber attack and should be included in the environment. As well, the domain may not be global, as in the case of mobile ad hoc networks. We therefore propose the following definition of the cyber environment: *A domain[4] within the information environment consisting of interdependent network information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers, and the software and information that reside within them.*

In this paper we consider operations in the cyber environment as a subset of information operations (IO) and can include elements of computer network operations, physical operations (i.e. land, air, maritime, space), psychological operations (PSYOPS), electronic warfare (EW), and Signals Intelligence (SIGINT). Computer Network Operations (CNO) is defined as "actions taken to defend, exploit and/or attack information resident on Information Systems (IS) and/or the IS themselves" (DND, 2009a, p. 37); and is comprised of the combined disciplines of Computer Network Defence, Computer Network Exploitation, and Computer Network Attack, where (DND, 2009b):

- Computer Network Defence (CND) is an activity conducted through the use of

2 The definitions are meant to provoke discussion, not to establish formal Canadian definitions. They do not represent the views of the DND/CF.

3 Domain in the US definition refers to an environment, whereas in this paper domain refers to a functional domain.

4 Domain is used here to align with the US definition.

one's own computer networks to protect, monitor, detect, analyze, and respond to unauthorized activity within computers or computer networks;

- Computer Network Exploitation (CNE) is a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and/or process information on computers or computer networks; and
- Computer Network Attacks (CNA) is a directed activity conducted through the use of computer networks to intentionally disrupt, deny, degrade, or destroy adversary computers, computer networks, and / or the information resident on them.

Like IO, cyber operations can be either offensive or defensive; we propose:

- Defensive cyber operations are *actions taken in the cyber environment to protect one's own information and information flow and maintain freedom of action in the cyber environment for friendly decision-makers.*
- Offensive cyber operations are *actions taken in the cyber environment to deny the actual or potential adversary's use of or access to information or information systems and affect their decision-making process.*

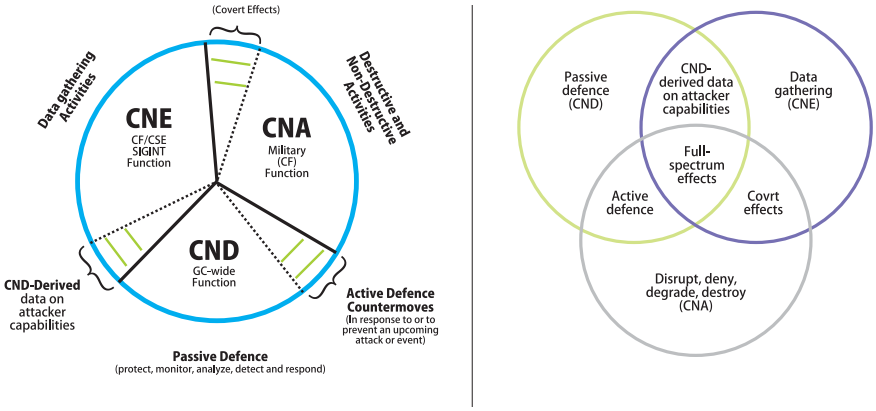

Figure 1. Current CNO model for the CF (left), and proposed model with overlap between CNO disciplines (right).

In the CF, the focus is currently on CNO because it is the main component of cyber operations and of the activities that form cyber operations, it is the least mature. Figure 1 (left) shows the current model of CNO in Canada, which was first introduced in January 2005 (Neasmith, 2005). This view can leave an impression that an operation may only be one of CNA, CNE or CND, and no overlap exists. We propose the Venn diagram shown in Figure 1 (right) because there are operations that can be simultaneously considered as CNA/CNE, CNA/CND, and CNE/CND, as well as CNE/

CNA/CND ("full-spectrum effects").

Below are examples of activities that could fall within the intersection of more than one CNO discipline (Castonguay, 2009):

- CND ∩ CNE: CND-derived data on attacker capabilities. CND contributes to CNE through deriving data about the attacker's capabilities from the sensor logs. Also CND monitoring activities may reveal unusual network activity that can help cue CNE activities toward a particular target.
- CND ∩ CNA: Active defence. CNA contributes to CND with active defensive countermeasures, where it may be necessary to counter-attack using CNA-type activities in order to protect the network.
- CNA ∩ CNE: Covert effects. Often CNA is required to gain access to a system for data gathering in CNE. Also the aggressive and covert nature of some CNE activities could be perceived as CNA in nature in the event that they are discovered.
- CND ∩ CNE ∩ CNA: Full-spectrum effects. An imminent attack requires a response that would be CND in nature but may require a CNA ∩ CNE technique such as insertion of malicious code.

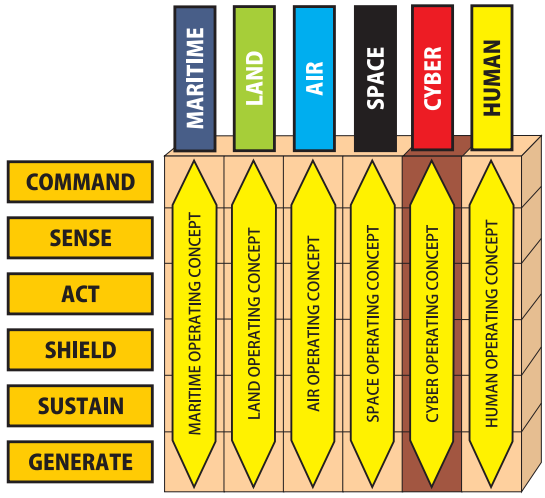

Figure 2. Capability matrix showing that capabilities can be viewed across functional domains or across environments[5].

5 This diagram is a modification of the Integrated Concepts diagram of the Integrated Capstone Concept document (DND, 2009c, p. 53).

It is also important to highlight that there exist strong interdependencies between the three CNO disciplines. For example, before you can attack a network you must first exploit the network and gather intelligence of that network in order to create your plan of attack. Similarly, before attacking a network you need to first protect/shield your network against counter attacks.

2. CYBER OPERATIONS WITHIN THE DND/CF CONSTRUCT

To assist in capability development and management, the CF uses six functional domains: Command, Sense, Sustain, Act, Shield, and Generate. These domain concepts are not mutually independent, but the interdependencies have not been studied in detail and are left to future work. Capabilities can be seen either from the viewpoint of the environment, or from the viewpoint of the functional domain, as seen in Figure 2 (DND, 2009c). In section 2.1, we examine the capabilities within the cyber environment across the functional domains. In sections 2.2 and 2.3, we examine how the capabilities within the cyber environment support the other operational environments, and how capabilities in the other operational environments support cyber operations. This is not intended to be a comprehensive listing of cyber activities but suggestions leading toward discussion and dialogue.

2.1 CYBER CAPABILITIES

2.1.1 Command Domain

In capability development, Command is defined as "The human dimensions of command embedded within competency, authority, and responsibility; the creative expression of human will necessary to accomplish a mission; the establishment of common intent; and, the structures and processes necessary to manage command. As an operational function, Command sits as the nexus for the four other operational functions [Sense, Act, Shield, and Sustain. (Generate was added later)]" (CFD, 2009). By being at the nexus for all other operational functions, it ensues that the Command domain is linked to many elements of cyber operations. Cyber capabilities in the other domains are discussed in their corresponding sections to follow.

Situational awareness of the battle space enables the C2 process. In the cyber environment, understanding the battle space requires situational awareness of all networks involved in operations. These include our own networks, service provider networks, as well as enemy networks. Information acquired about these networks by using CND and CNE sensor technologies must be fused together into a Common

Operational Picture (COP) to give the commander an understanding of the cyber battle space within his operation. Knowledge of the adversary's CNO capabilities, (e.g. cyber weaknesses, and CNA capabilities) will allow for the targeting of enemy assets in the cyber battle space. Additionally, for international operations, sharing cyber information in a multi-national COP enables coordination and improved defence for all nations involved.

2.1.2 Sense Domain

The sense domain is defined as "A single comprehensive entity that collects, collates, analyses, and displays data, information, and knowledge at all levels. Tactical, operational, and strategic assets are integrated into a single continuum." (CFD, 2009) In the cyber environment, intelligence, surveillance and reconnaissance (ISR) may be obtained using CND, CNA and/or CNE activities and the dissemination of all ISR is enabled by CND.

The essential capability of the Sense domain is to provide the decision-maker with intelligence information that has been assessed and interpreted in the proper context (Fong et al, 2009). The first step is defining the information required by the decision-maker with respect to the cyber environment. The information required needs to answer questions like (note that this is not an exhaustive list):

- What are the threats/risks to my network? Are there indications that an attack is pending or in progress? From whom?
- What on my network is critical to my operation? Is its confidentiality, integrity or availability vulnerable to an attack?
- What do we know about the enemy's capabilities and location in the cyber environment?

The raw information pertaining to one's own network can be obtained by using a variety of tools that give a picture of the real-time structure of the network, and the activities taking place upon it, including known patterns of attack. When an attack is detected, the threat agents and their locations in the cyber environment can be marked for special attention. Open Source Intelligence (OSINT) data can be obtained from publicly available Internet sources for technical information regarding vulnerabilities.

Information about the adversary's networks and the Internet at large can be obtained using passive traffic analysis techniques and other active probing tools (CNE activities). It is important to understand the enemy's cyber vulnerabilities and the criticality of their network assets (Leblanc and Knight, 2005a). This may require penetration of the network to give visibility behind routers and firewalls. Signals Intelligence (SIGINT) data, processed from intercepted network traffic, can also give

a picture of the structure and activities of the enemy's networks. Over time, information can be collected from CND sensors that can reveal patterns in the enemy's tactics and assets. Information can be acquired about an attacker's goal, objectives and capabilities by using network counter-surveillance operations where the attacker is allowed to continue the attack in a risk-managed environment where his actions are observed (Leblanc and Knight, 2009). CNA methods can cause the enemy to react to a cyber attack, thereby revealing their capabilities in the cyber environment (Leblanc and Knight, 2005a). Human Intelligence (HUMINT) can be applied via infiltration of the Black Hat (unethical hacker) community, and OSINT via publicly-available Internet sources for both technical information and for actors.

2.1.3 Act Domain

In capability development, Act is defined as "The use of a capability to influence events across the spectrum of conflict and in either or both of the physical and moral domains. Act reflects an integration of capabilities from a variety of sources – tactical, operational, or strategic." (CFD, 2009) Assuming that the activities that can be carried out to produce effects in the cyber environment are entirely within the auspices of CNA, the activities are limited to operations that deny, degrade, disrupt or destroy the integrity, availability or accessibility of information on the enemy's systems.

Some examples of how the enemy may be engaged (in the cyber environment) to produce effects in the cyber environment are (modified from Leblanc and Knight (2005a, 2009)):

- Create a virtual diversion to occupy the focus of the enemy command and control.
- Degrade the network-based communications systems of the enemy.
- Deny a secure communications service so that unencrypted communications must be used.
- Modify information in the cyber portion of the enemy command and control systems to mislead them into, or keep them in, a vulnerable position.
- Insert false information on a friendly system in order to allow the enemy to find it during an enemy reconnaissance activity.
- Penetrate and gain control of an enemy's weapon system and use the system against it.

2.1.4 Shield Domain

The Shield functional domain is defined as "Force protection measures taken to

contribute to mission success by preserving freedom of action and operational effectiveness through managing risks and minimizing vulnerabilities to personnel, information, matériel, facilities and activities from all threats." (CFD, 2009) The primary cyber operations in the Shield domain are CND operations, and it refers only to the protection of network assets.

An effective and efficient Shield capability requires situational awareness (SA) of the cyber environment including IT infrastructure, security alerts, vulnerabilities present on the network, and what each asset on the network is being used for, all of which comes from Sense domain capabilities. Assessment of threats posed by the enemy's cyber capabilities may already be available from the processed Sense data. When threats and vulnerabilities have been assessed (i.e. processed relative to the criticality of the exposed and vulnerable devices and relative to the capabilities of the enemy) proactive remediation (e.g. application of patches) can begin as a proactive Shield capability.

When an attack has been detected, for example through an intrusion detection system or advanced traffic analysis, defensive measures can be taken. Depending on the nature of the attack, the response may be:

- Physically unplugging the target device.
- Blocking related traffic using a firewall.
- Redirecting the attacker into a "honeypot" to observe their techniques and intent (Leblanc and Knight, 2005b), or conducting network counter-surveillance operations (Leblanc and Knight, 2009).
- Conducting CNA to disable the attacker.

The recovery process may require: restoring a device from a known clean backup image; decontaminating one or more hosts from a virus infection; and investigating possible changes to prevent a second occurrence of the attack.

The human aspect of defending against threats involves educating users about the role that they play in the security of the network, and the potential real effect of disregarding security procedures.

2.1.5 Sustain and Generate Domains

In capability development, Sustain is defined as: "A grouping of all functions necessary to generate, deploy, employ, and redeploy a force. As an operational function, the term is to be taken in it broadest possible context. Sustainment concerns are loosely grouped into three subordinate functions: materiel, personnel, and engineering." (CFD, 2009) In the cyber environment, Sustain is the capability to maintain the

networks, which consists of the cyber capabilities found in the Shield domain. The CF's ability to meet these demands is not a question of mandate but one of resources (Castonguay, 2009). As for all capabilities, personnel resources are key to their sustainment; however, the fast rate of change of technologies in cyber capabilities leads to difficulties in differentiating between Sustain and Generate (Castonguay, 2009; Allen, 2002).

Generate is defined as "The process by which military forces are assembled, equipped, trained, certified, and deployed to meet a force employment requirement." (CFD, 2009) In order to meet the requirements of the cyber environment it is important to hire and retain the right people with the right capabilities for the entire CNO spectrum (to conduct CNA/CNE/CND). The personnel resources required to support cyber capabilities need a high level of expertise in their field, which is not supported by the CF's career management cycle where personnel are rotated every two to four years. Therefore, by the time military personnel have gained enough expertise to be proficient in their role it is almost time for them to move on to their next post (Castonguay, 2009). As we move towards more network-enabled the need for cyber expertise will increase and due to the fast rate of change in cyber technologies, training becomes an almost constant requirement. This highlights the importance of retaining these individuals and consequently the need for revising the career management structure for the cyber-trained military personnel.

2.2 OTHER OPERATIONS SUPPORTED BY CYBER CAPABILITIES

Capabilities used in full spectrum operations conducted in the traditional environments are often supported by cyber capabilities (mostly through CND). Current and future operations in general are heavily based on information. Having the right information at the right time implies that the information required for the decision process must be available, its transmission confidential, and it must be stored in such a way as to ensure its integrity. Sharing information with a COP, whether nationally or with allies, requires secure communication and storage to ensure confidentiality, integrity and availability, which is enabled by CND capabilities.

The planning of operations is also enabled by CNA/CNE capabilities. Through CNE, intelligence information about an adversary's plans may be obtained if they are stored on a computer. Planning is enhanced with knowledge of the adversary's CNO capabilities, for example, knowledge of the enemy's cyber weaknesses, and what their CNA capabilities are, including whether they could produce effects in the physical environments. If the network could be penetrated as far as the enemy C2 systems, one could access their operational plans and commander's intent. This

knowledge could also be gained by using network counter-surveillance operations (Leblanc and Knight, 2009). Such information comes from the Sense domain and directly influences the decision cycle. The cyber environment also contributes CNA to the arsenal of weapons from which the commander can choose when forming a plan. CNA capabilities were discussed under the Act domain. The cyber environment also enables the social networking required to plan operations among individuals at different locations by providing software and mobile devices.

In the psychological space, one may influence behaviour by dispersing information via Internet radio, web sites, e-mail. One may send false information by using these same avenues. Denial of service tactics can be used to deny or disrupt information to the enemy, and one can provide alternate routes to the Internet to those for whom Internet access has been blocked. The recent incidents in Iran are an example, as well as Burma (Diebert and Rohozinski, 2009).

The availability of networks and the Internet enables many other functions required for planning operations. For example, the availability of online services and remote access to resources allows for the use of the cyber environment for recruitment, training, and procurement.

2.3 CYBER OPERATIONS SUPPORTED BY OTHER CAPABILITIES

Similar to how cyber operations can support capabilities within other environments, the reverse is also true: cyber effects can be supported or delivered by capabilities that exist within the other environments. Some examples of how the enemy may be engaged in the other environments to produce cyber effects are:

- Kinetic means: using kinetic weapons either land, air or sea base to destroy servers and/or communications link thus denying/limiting the enemy access to the cyber environment.
- Implanting cyber spyware: in order to implant hardware such as a network taps or keyboard sniffers on enemy networks, the use of Special Forces may be required to physically implant the devises.
- EW capabilities: using electronic attack techniques, such as jamming or electronic deception, to deny enemy access to wireless network devices and command and control systems or to confuse enemy ISR systems.
- PSYOPS capabilities: using social engineering techniques to encourage the enemy to disclose network information or inject malicious code, e.g. obtaining

passwords.

- C4ISR capabilities: Intelligence collected through conventional means (e.g. SIGINT, Intelligence report) can contain information about the people, e.g. those involved in a terrorist group's social networks.

3. CHALLENGES

There are two root causes of major challenges that will have to be addressed to advance cyber operations. First, the environment in which cyber operations take place is far more dynamic than the physical environments. Actions in the cyber environment can literally take place as fast as the speed of light, and technologies evolve very quickly, relatively to technologies in other environments (e.g. Moore's Law). Second, the cyber environment is indistinct in terms of boundaries, be they physical, political, socio-economic, or otherwise. Both of these characteristics lead to challenges that are more problematic in cyber operations than in other types of operations.

The production of policies and legislation is a challenge in both areas. Policymakers at all levels need to be conscious that the mechanics of cyber operations will require changes in the policy realm. This implies a commitment to provide those policymakers with the necessary education to raise awareness. Scientific support through an advisory role can enable good decision-making in both policy and cyber operations.

3.1 DYNAMIC ENVIRONMENT

The dynamic nature of the cyber environment leads to challenges in operations; for example in defensive operations software vulnerabilities are announced faster than they can be addressed. Similar examples can be found in other types of cyber operations. This can be addressed by increasing the number of personnel with specialized training, all of whom will need continuous training to keep abreast of changes in technologies (e.g. vulnerabilities) as they evolve. Continuous education and security awareness is also required for end-users; research into the human aspects of cyber security is sparse and should be augmented to yield more useable security technologies and processes.

Because of the rate of change in technology and the speed at which actions occur, the challenge lies in our capability to minimize risk and respond appropriately to an attack. For this, we will need to have a dynamic threat and risk assessment rather than the static ones used today, and dynamic situational awareness of our networks and how they are being used operationally. Research and innovation is needed to

produce technologies to automate the laborious and complex task of a complete network risk assessment that includes the operational consequences of an attack.

New infrastructures will be required that will promote the agility and flexibility of our forces, as required by the Canada First Defence Strategy (DND, 2008). Because new technologies are being developed at such a fast pace, these infrastructures must be built in such a way that their implementation can be done in the least disruptive manner possible.

The policy realm also faces challenges due to the dynamic nature of the cyber environment. Scientific and technological advances are moving faster than the accountability and responsibility control mechanisms, and faster than the ability to implement public policy and legislation.

3.2 UNDEFINED BOUNDARIES

The Internet was built to be resilient to outages. Redundant routes are introduced to ensure that there is always a path connecting any two nodes. The downside to this design is that these networks are all connected: one poorly secured network introduces a risk to all other networks. Detection of the proliferation of hostile technology, intent and behaviour is more complicated due to the extent of the cyber environment. Even when a threat is detected, preventive actions (both in the physical and cyber environments) are difficult due to legislative context, anonymity of the users, and the use of free hosting services. A central regulating agency to monitor the cyber environment, national or global, would improve threat detection. With a national regulatory agency, a nation can monitor activities within their own borders (as ill-defined as they are in the cyber environment); however, excessive regulation will likely not be possible due to the commercial aspects of the Internet. On a global scale, a central regulating agency would enable the creation and enforcement of international cyber laws. Clearly, this will present a major challenge in the global policy and legislation realm.

In the cyber environment, it is very difficult to positively attribute an activity to a person or nation, or to a physical location. If we could positively attribute an attack to a nation, this could constitute an act of war. In this case, we have to be prepared for cyberwarfare, which will require development of policies, legal frameworks and procedures with respect to these cyber capabilities. Policy for CNE/CNA activities outside of one's own network boundaries is currently undefined and is a potential barrier to CNE/CNA in cyber operations. As an example, portions of the Internet are owned and controlled by privately owned Internet Service Providers, who may object to surveillance activities being carried out via their property. In cyberwarfare, it must be recognized that actions taken will leave the boundaries of the virtual

world and have effects in physical and cognitive/human space. There needs to be an augmented Sense capability that can assess these nonphysical effects. As well, a change of mindset is required when approaching effects assessment. This requires ways of applying the same notions of detecting, identifying, classifying, etc., to non-physical effects. Research in cyber, cognitive, and social systems may provide some insight in how to do this.

Another challenge stemming from the lack of boundaries in the cyber environment is information sharing. Departmental policy frameworks and behavioural norms lag behind the requirement to share and exploit information. The institutionalization of restrictive policies and barriers concerning information and intelligence is a result of the mindset of "need to protect" rather than the more productive "need to share". The risk is that necessary information will not get to the right people at the right time, and that they will remain information "deprived" and therefore unable to obtain situational awareness and consistently engage in effective decision-making. To mitigate the risk of leakage of sensitive information, policies and procedures must be developed to ensure that the right information is shared with the right people, on a regional, national, and global scale. Research and development could help to determine the information required for good decision-making.

Once the information sharing policies are in place, a common network and/or an effective information sharing capability is required, both within a nation and between nations. The establishment of trusted networks or enclaves with secure identity and access management will encourage users to collaborate and share information in a secure environment. Some countries, e.g. Australia, have established this national capability. In the CF, there is a need for the design and development of command and control systems that integrate cyber situational awareness with other operational awareness. These systems must be interoperable with OGDs and agencies, NGOs, and allied systems. Interoperable standards and common exchange formats to support exchange of SA information, when and if authorized, have not been agreed upon; this will take time to develop into policy. There are also legislative limits on how the CF can handle information gathered while conducting CNE types of operations, e.g. privacy rights.

4. DISCUSSION

The sections above demonstrate that cyber operations are ubiquitous. The cyber environment as a battle space will consist of joint cyber operations that touch all of the other environments (land, sea, air, space, human/cognitive) by producing effects in these environments or by acting as a supporting element in a joint campaign plan. Likewise, operations in the traditional environments can support and provide

capabilities to cyber operations.

It was previously described that CNA, CNE, and CND are closely coupled. As a result, they cannot be categorized individually into the functional domains. For example, CND does not exclusively fall under the Shield domain, CNA under the Act domain, and CNE under the Sense domain. CNO has links into each of the six functional domains. It can be both a capability and a support element. Figure 3 illustrates the relationships (as capability or support links) between CNA, CNE, CND and the six functional domains of Command, Sense, Act, Shield, Sustain, and Generate, as described in the above sections. A dashed line indicates that a CNO element is supporting a domain, and a solid line indicates that a cyber capability exists in a domain.

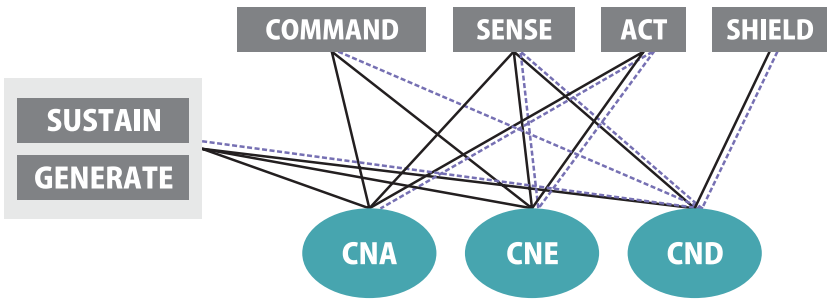

Figure 3. CNO and Functional Relations. The solid lines indicate that a cyber capability exists in a domain, and a dashed line indicates that a CNO element is supporting a domain.

The complexity of the interdependencies between cyber capabilities, the CF's functional domains, and the other traditional environments supports the position that the cyber environment should be treated as an independent battle space with its own inherent capabilities. In addition to those described in section 3, it also gives rise to challenges in operating in such an environment: doctrine and ownership issues result in duplication of effort, which ultimately costs money.

CNO capability development is currently grouped under C4ISR in the CF's C4ISR Capability Development Plan (DND, 2009a). Although the CF recognizes that CNO, and consequently cyber operations, are more than C4ISR and that these operations span a number of domains, senior leadership gave direction that CNO and cyber-related issues be brought forward though the Command domain as a primary reporting mechanism. This mechanism provided a way forward for the development of new draft polices for CF CNO (currently in review), and the initiation of a CNO strategy (in development). The same is needed for cyber operations. Considering cyber operations as CNO and having CNO as an element of C4ISR is not conducive to force development in the cyber environment. The CF needs to establish an organizational

infrastructure to address cyber-related issues and programs.

The CF is making progress towards this goal. Since this work began, it has been proposed that a cyber task force be established by summer 2010 to address cyber force development and generation, and to establish a cyber domain with inherent network exploit and network attack/effects capabilities (BGen S. Noonan, personal communication, 2 February, 2010). This is an important development because treating the cyber environment as a battle space will challenge current doctrine and will involve further concept development and experimentation. A cyber strategy and campaign plan will need to be developed, followed by concepts and doctrine for cyber operations.

As cyber attacks can target critical infrastructures and citizens, a whole-of-government approach will be needed to develop cyber policies and capabilities in a coordinated manner. There are several key players in cyber operations at the whole-of-government level, each of which has a mandated area of responsibility. The interrelationships of these mandates can be extremely complex. Consequently, depending on the type of cyber activity, the CF may or may not play a lead role. Concept and doctrine development, as well as policies, within the CF must reflect this change of mindset. Without a whole-of-government approach, the CF will not be able to effectively fulfil its mandate to defend Canada in the cyber environment.

On the research and development side of DND/CF, there are currently initiatives in developing a CNO Science and Technology (S&T) Strategy that will guide S&T efforts supporting the development and sustainment of cyber capabilities of the CF, and exploring the aforementioned cyber effects.

REFERENCES

- Allen, Maj F.J., 2002. CN(EH?) – *A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities*. CSC 28 Thesis, Canadian Forces College, Toronto.
- Castonguay, LCol F., 2009. *Evaluating Canada's Cyber Semantic Gap*. JCSP 35 Master of Defence Studies Research Project, Canadian Forces College, Toronto.
- Chief of Force Development (CFD), 2009. *Capability Domains – Definitions*. Retrieved 1 May 2009, from DND intranet http://cfd.mil.ca/sites/page-eng.asp?page=4281.
- Department of National Defence, 2008. *Canada First Defence Strategy*.
- Department of National Defence, 2009a. *C4ISR Capability Development Plan*.
- Department of National Defence, 2009b. *Canadian Forces (CF) Computer Network Operations (CNO) Policy Draft Version 2.1*.
- Department of National Defence, 2009c. *Integrated Capstone Concept Draft*.
- Diebert, R., Rohozinski, R., 2009. Ottawa needs a strategy for cyberwar. *Information Warfare Monitor*. Retrieved 8 February 2010 from http://www.infowar-monitor.net/2009/06/blog-1/
- Fong, V., Cantlie, C., Farrell, P., Geling, G., Hughes, S. (2009). *Capability Domain Concept Sense Capability Domain*. Defence R&D Canada - Center for Operational Research and Analysis, DRDC-CORA-TM-2009-026.
- Leblanc, S. P., Knight, G. S., 2005a. Information Operations in Support of Special Operations. In D. Last and B. Horn (eds.), *Choice of Force - Special Operations for Canada* (pp. 173-185). Montreal: McGill-Queen's University Press.
- Leblanc, S. P., Knight, G. S., 2005b. *Engaging the Adversary as a Viable Response to Network Intrusion*, Workshop on Cyber Infrastructure – Emergency Preparedness Aspects, University of Ottawa, Ottawa.
- Leblanc, S. P., Knight, G. S., 2009, *When Not to Pull the Plug – The Need for Network Counter-Surveillance Operations*. In Czosseck, C. & Geers, K. (eds.), The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 226-237), Amsterdam: IOS Press.
- Neasmith, Col. D., 2005. *CNO: Considerations for DND/CF Requirements*. Retrieved 3 February 2010, from http://www.afceaottawa.ca/uploads/CNO%20Briefing%2011Jan05.ppt
- US Department of Defense, 2009. *Joint Publication 1-02 Dictionary of Military and Associated Terms*. Retrieved 7 February 2010, from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

KEYWORD INDEX