ENEKEN TIKK ANNA-MARIA TALIHÄRM
(EDITORS)

INTERNATIONAL CYBER SECURITY

LEGAL & POLICY PROCEEDINGS

2010

Publisher:
CCD COE Publications
Filtri Tee 12
10132 Tallinn
Estonia
Tel: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
www.ccdcoe.org

Printed By: EVG Print
Design & Layout: Marko Söönurm

ISBN: 978-9949-9040-4-4

ENEKEN TIKK
ANNA-MARIA TALIHÄRM

LEGAL & POLICY PROCEEDINGS 2010

2010

CONTENTS

INTRODUCTION

Col Ilmar Tamm

To introduce the proceedings of the Legal and Policy Track of the CCD COE Conference on Cyber Conflict 2010, I have borrowed the "fog and friction" motive from General Clausewitz[1]. I have done so not only because as a military commander I value the experience and guidance of the classics, but also to highlight one of the fundamental questions about the applicability of "classical" military approaches to contemporary cyber defence and security.

To further illustrate the overall military approach that underlies my line of thought, let me begin with assuring that military leaders, lawyers and policy experts all struggle with how much of the existing theory and practice could be adapted to the new dimension of cyber threats, and at the same time aim to identify the loopholes that require new solutions and approaches.

Having observed the landscape of global cyber security forming its shape over the past few years, I would characterise the current phase of development as "aware but confused". Compared to three years ago, cyber threats are much more acknowledged as part of our national security concerns. However, a complete understanding of the threat and effective defences are yet to be developed.

At the time Clausewitz concluded that friction is the difference between "war on paper" and actual military action, the term "war" entailed a lesser degree of political perspective than it does today. Therefore, in the context of cyber space, I knowingly employ the notion of "war" in a very liberal meaning not having much regard to the legal and policy ramifications of a "cyber war".

I argue that "total cyber defence" encompasses the utilization of all available resources in order to maintain an organized, functional society and to protect the population and national assets thus being the sum of individual defence efforts of numerous stakeholders, each of them embracing to an extent a different threat picture and specific capabilities. Similarly, the legal approach to cyber security considers the wide range of variations of a cyber conflict: the information security

1 This and other interpretations of General Clausewitz's theory are developed on the basis of: Carl von Clausewitz. On War. http://www.clausewitz.com/readings/OnWar1873/TOC.htm.

aspects, criminal attempts and their motivation, national security relevant intrusions and, ultimately, acts of cyber warfare. Consequently there is no effective way for a single state, institution or discipline to defend against all possible cyber threats in isolation. This is due to the architecture of information and communication systems as well as the interdependence of private and public information services and systems that requires cooperation and coordination on multiple levels of management.

Developing a coherent cyber security approach starts with an understanding of the entire threat picture, which in cyber space appears to be similar to a three-dimensional puzzle. Besides "business as usual", one needs to be aware of the political, geographical, demographical, historical, sociological, etc. context to which the threat belongs, taking into account the characteristics of the victim state (that is, e.g., why Estonian banks and online media fell under a cyber attack in the context of the Bronze Soldier Riots) as well as the unique elements of the attacks, such as their origin and threat vectors (e.g. patriotic hacking). On top of that, as underlined by T. Wingfield and E. Tikk in their article "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen", all cross-border incidents are to a greater or lesser extent affected by the actors' international relations and the stance of the international community.

To explain how cyber security and defence planning differs from traditional military planning, I have used the Borg Summary of the Cyber-Defence Revolution where he characterises the essential differences between cyber defence efforts and industrial defence. According to Borg, cyber defence is concerned with having to defend against networked groups often not clearly connected to nation states; diffusing forces potentially scattered around multiple jurisdictions in all seven corners of the world and thus requiring ubiquitous force to respond; and the advantage of information over fire power.

This affects our strategy and tactics. Strategically, it is a lot less about geographical defence perimeters and outside threats as the targets include internal networks and inside attacks. Targets have transformed from military-industrial into often privately owned critical infrastructure. The obvious effect of an attack is no longer primarily measured by referencing injuries, death or physical destruction. Instead, the price of the protection and destruction of a certain information asset is evaluated by the influence it has on the functioning of a society or a nation. Nevertheless, injury and death as well as physical destruction may also be the direct causes of a cyber attack.

Therefore, battlefield theories need to undergo the test of economic theory – even with more than 2% of Gross National Product spent on national defence no government is able to reach the level of security needed to completely secure

national cyber interests.

Furthermore, Borg claims that we have moved from deterrence-based policies to the era of resilience-based policies. I would argue that a good defence concept still produces a great amount of deterrence and conclude that we need to keep both ends in mind when drafting our cyber security approaches.

Turning to the tactical level, we are facing the interrelation of integrated systems with extensive automated programs, complex repositioning, information systems turned into weapons, co-optional systems and process targeting. And although the success of an attack is probabilistic from the attacker's point of view, the same probability should and is driving defence planning and investments. Thus, expectation has a different meaning in cyber defence – to expect a cyber attack literally means to hit the security jackpot.

This all affects how decisions are made about developing and sustaining information superiority – a term that comprises the confidentiality, integrity and availability of information in the widest possible sense. Due to the multiple stakeholders in charge and their effective control over individual components of the information infrastructure decision-making is inherently distributed.

All planning occurs in the context of uncertainty about the identity of the adversary, difficulties in recognising patterns and distilling useful information out of noise. Reaction has a different meaning in cyberspace – only technology can keep up with technology.

Consequently, even from the merely theoretical perspective preparing against a cyber attack is most challenging. Once you see it coming, your adversary sees you see it coming, whereas repositioning the attack is significantly more convenient than repositioning your defence investments.

It is not difficult to picture a possible cyber threat – it is a monstrous cyber-evil with a minimum of three heads and at least four arms, all fully loaded, quick, smart and agile. And because it has advantages over human decision-makers, it is often problematic to figure out where it will hit next. It might well be that Clausewitz's assessment - that a successful defence is easier to achieve than a successful attack: provided both parties possess equivalent capabilities - is not true in cyber conflict.

With all possible means, targets, actors and effects cyber defence may look like a mission impossible from every single point of view. That is why the combination of critical viewpoints and interdisciplinary approaches creates the best premise for defence.

When refining the monstrous threat picture, learning from the past is easy,

but ineffective. Asymmetric threats are about unpredictability and targeting the weakest link of the chain. Therefore, the links you have reinforced based on experience mark just the beginning of your defence effort. Accordingly, to ensure that one's cyber defence effort is effective, one needs to maintain both full awareness of the present danger and threat picture as well as the ability to extract future trends out of previous experiences and current visions.

In order to determine which points are critical, one has to look at the criteria such as business purposes, decision-making processes, critical nodes of the society and economy, role of the information infrastructure for government and civil society purposes and also geographical locations and political alliances. This will determine realistic threat vectors.

Filtering out realistic and target-specific threats should result in developing a more clear understanding of the allocation of defences: the resources and effort to be invested by a specific entity associated with those available and coordinated on national and international level.

In the longer run, elimination of impressions and the fog resulting thereof will facilitate developing cyber security niches, i.e. unique defence attention areas with timely action and links to adjacent areas of responsibility. This means a better understanding of what organisations such as NATO, UN, the European Union and others can provide for nations, what our countries can provide for us and what we can provide to national cyber defence.

After defining the threat picture, the question of what can every stakeholder effectively contribute to support national, NATO, and global cyber security while focusing on securing its primary services and systems remains. We are all experienced in securing "our portion of cyber space", but we need to decide on how to effectively control cyber space as a whole.

As we have learned from the past few years cyber crime is the most common challenge to our way of life in the information society. Therefore, there are steps that need to be taken at the end-user level with the help of Internet infrastructure providers. The fact that cyber crime has obtained a political context forces us to review our criminal policy in the field.

A great challenge for the government is to understand where security investments of the private sector could potentially support national cyber security efforts (e.g., how should information about cyber incidents be available to CERTs and where certain services could be sacrificed to support the availability of critical functions). It is also necessary to decide on a national level how to orchestrate coordination, or even achieve cooperation between governmental agencies involved in the field

of cyber security.

From military point of view, there are few purely military functions that can be put in practice in a contemporary cyber conflict. Military responses to cyber incidents remain one of the least defined and at the same time legally most ramified remedies.

Hence, total defence in cyber context means getting rid of a stove-piped approach to cyber security planning and strongly encouraging synergy between information society design, criminal policy planning, law enforcement capabilities and military defence. Additionally, as suggested by M. Dion in her article "Different Legal Constructs for State Responsibility", the novel nature of cyber defence demands the review of several traditional domains such as the legal aspects warfare and state responsibility.

To add one more dimension to the thinking about effective cyber security, I use the concept offered by Professor Thomas Wingfield and developed by a team of legal experts at the CCD COE 2009 Legal and Policy Conference. Seen in the DIMPLE context, law is but one aspect of cyber incident management. Thus, potential remedies as well as challenges related to cyber incident management may exist in the diplomatic, intelligence, military, policy or economic context. Keeping this in mind and acknowledging the role of each individual discipline in a holistic approach will over time empower us in the defence against cyber attacks.

As Clausewitz has observed, a general in time of war is constantly bombarded by reports both true and false; by errors arising from fear or negligence or hastiness; by disobedience born of right or wrong interpretations, of ill will, of a proper or mistaken sense of duty, of laziness, or of exhaustion; and by accidents that nobody could have foreseen. In short, he is exposed to countless impressions, most of them disturbing, few of them encouraging. In a cyber conflict, this challenge is exacerbated by the fact that attacks are rather easy to launch, defence is times more costly than attack, states often choose to ignore or even nourish cyber perpetrators in their jurisdiction and because of our way of life, we are growingly vulnerable to these attacks.

In an age waging an effort to solve "the secret of the universe" it may be easy to believe that it is difficult to say something new, and it may seem that we know it all and nothing can surprise us. This may create "the illusion of security" – and exactly that was, by the way, the Estonian mindset before the 2007 attacks. Cyber threats are threats targeted against our comfort zone. And looking critically at what we think we know will help us beat a big part of the misconception of security.

As I mentioned earlier, cyber security with all its challenges and dilemmas forms a complex puzzle. Fortunately, it is a puzzle that can be solved. This book offers only

a glimpse of all the debates that were raised during the conference and touches upon substantial topics reflecting the current state-of-the-art of cyber security.

I believe that this book is a small but considerable step towards a better understanding of the challenging symbiosis of cyber security that is framed by the triangle of law, policy and technology.

BIOS

Maeve Dion

is currently Doctoral Candidate at Stockholm University. Before starting her studies in Stockholm, Maeve worked as the Program Manager for Education and Cyber, Centre for Infrastructure Protection & Homeland Security, George Mason University School of Law, Arlington, Virginia, USA. Her work focused on legal, policy, economic, and educational issues relating to critical infrastructure protection, particularly information infrastructure. Ms Dion manages the Centre's educational programs, which include work with DHS on infrastructure protection programs in higher education. Maeve's other areas of research include the national security concerns of foreign access to and control of critical infrastructure, and the relationships between military and civilian authorities regarding security and defence of critical infrastructures. Ms Dion is an invited academic expert to task forces of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC). She is also principal investigator of a legal study for the Cyber Conflict Studies Association (CCSA); part of CCSA's 2009-2011 research agenda. Ms Dion holds an honours B.A. in political science from Eckerd College, and a J.D. cum laude from George Mason University School of Law.

Ulf Häußler

is currently working at the U.S. National Defence University, is a member of the Legal Service of the German Armed Forces since 2002, following a period as a research fellow in international law at the University of Konstanz (1998-2002). 2009-2010, he was seconded to NATO to serve as Assistant Legal Advisor Operational Law at Allied Command Transformation. He has been deployed to KFOR (2006) and SFOR (2004) and has also served on secondment in the Legal Office, NATO International Staff (2006). He is a member of the editorial board of The Military law and the Law of War Review and has published on the law of international military operations.

Daniel J. Ryan

is a Professor of Systems Management at the National Defence University, teaching

information security, information assurance, cryptography, network security and computer forensics. Prior to joining NDU, he was a lawyer in private practice, a businessman and an educator teaching law and information security for George Washington University. Prior to entering private practice as an attorney, he served as Corporate Vice President of Science Applications International Corporation with responsibility for information security. Prior to joining SAIC, Mr Ryan served as Executive Assistant to the Director of Central Intelligence. Earlier, he was Director of Information Systems Security for the Office of the Secretary of Defence serving as the principal technical advisor for all aspects of information security. He developed information security policy for the Department of Defence and managed the creation, operation and maintenance of secure computers, systems and networks. Mr. Ryan received his Bachelor's degree in Mathematics from Tulane University, a Master's in Mathematics from the University of Maryland, a Master of Business Administration degree from California State University and the degree of *Juris Doctor* from the University of Maryland. He is admitted to the Bar in the State of Maryland and the District of Columbia.

Julie Ryan

is the Associate Professor and Chair of Engineering Management and Systems Engineering at The George Washington University. Her research interets are mathematical modelling approaches to complex information security challenges, multi-disciplinary approaches to complex infosec problems that integrate operations research and systems engineering, the application of multi-attribute utility theory to architecting holistic information security solutions and information warfare theory and applications. Her current projects include being a member of the Board of Directors at the Colloquium on Information Systems Security Education and a member of the Homeland Security Policy Institute (HSPI) Working Group on the Internet and Radical Factions.

Eneken Tikk

is Doctoral Candidate at Tartu University and the acting branch chief of Law & Policy branch in the NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Her research interests include legal-tech-policy dimensions of cyber security and interdisciplinary responses to global cyber threats. Ms Tikk is a legal expert on personal data, databases, and public information law. She was the head of the Cyber Defence Legal Expert Team at the Estonian Ministry of Defence; adviser on information law and legal policy to the Estonian Ministry of Justice. Among

other things Ms Tikk led preparations for the 2nd Data Protection Evaluation for Schengen Information System for the Estonian Ministry of Justice, and she has acted as the legal expert to the E-Health Information System for the Estonian Ministry of Social Affairs. Ms Tikk is the founder of the Estonian IT Law Association and the DLL IT and Media Law Institute. She received her B.A. in Law from the University of Tartu, her Magister Juris from the University of Tartu, and she is currently pursuing a Ph.D. in Law at Tartu University, with a focus in Information Technology and Cyber Defence law. She is the author of "Information and Law" textbook (in Estonian), the Frameworks for International Cyber Security compilation, and has co-authored "International Cyber Incidents: Legal Considerations" with Kadri Kaska and Liis Vihul.

Thomas C. Wingfield

is the Professor of International Law at the George C. Marshall European Center for Security Studies. Prior to his arrival at the Marshall Center, Professor Wingfield was deployed to Afghanistan as the civilian rule of law advisor to Gen. Stanley A. McChrystal's Counterinsurgency Advisory and Assistance Team from October 2009 to February 2010. He has worked as a national security attorney and an Associate Professor at the U.S. Army's Command and General Staff College at Fort Belvoir, Virginia, with a focus on operational law. Mr Wingfield has served as a Lecturer in Law at Catholic University, an Adjunct Professor at the Georgetown Public Policy Institute, and an Adjunct Research Fellow at the Potomac Institute for Policy Studies. He holds a J.D. and an LL.M. from Georgetown University Law Centre, and is completing an S.J.D. at the Law School of the University of Virginia. A former Chair of the American Bar Association's Committee on International Criminal Law, he is the author of The Law of Information Conflict: National Security Law in Cyberspace.

Kadri Kaska

holds a Master of Arts degree in law from the University of Tartu, Estonia. After eight years in the national communications agency, dealing with regulatory issues such as resource and infrastructure management, advising in the market regulation process, and being involved in the drafting of communications legislation, she joined the Cooperative Cyber Defence Centre of Excellence in 2008 and currently works there as a legal analyst. Her research interests include legal and economic aspects of cyber security, legal factors involved in cyber incident trend evolvement, and cyber crime. Kadri has co-authored "International Cyber Incidents: Legal Considerations" with Eneken Tikk and Liis Vihul.

Anna-Maria Talihärm

is working in the Cooperative Cyber Defence Centre of Excellence (CCD COE) Legal and Policy Branch. She is currently striving for a PhD degree, specialising in legal framework for cyber crime, and obtained her LLM degree in IT law from Stockholm University. After studies in the Voronezh State University, Russia and Paris VIII Saint Denis Vincenne University in France, she received her Bachelor's Degree from Tartu University Law Faculty. In CCD COE her areas of research include European Union information society law, data protection, cyber terrorism and cyber crime, and she has been involved in projects with COE DAT, ENISA, OSCE and ELSA. Anna-Maria has also been giving lectures on legal aspects of cyber security in Tallinn Technical University and Estonian Information Technology College.

FRAMEWORKS FOR INTERNATIONAL CYBER SECURITY: THE CUBE, THE PYRAMID, AND THE SCREEN[2]

Thomas C. Wingfield[3], Eneken Tikk[4]

INTRODUCTION

In the myths of ancient Greece, Heracles encountered the evil innkeeper Procrustes, who stretched short travelers and chopped off the legs of tall travelers to fit the fixed length of his guest bed. His name survives today as an adjective describing one-size-fits-all approaches to complex problems. As cyber security has grown into an international and multi-dimensional concern, this article proposes to avoid a procrustean approach to this sophisticated set of problems.

The complexity of cyber incident management has lately been addressed by both national and international regulatory and policy authorities. The national security concerns accompanying trends like patriotic hacking and political context of cyber incidents have forced governments and international organizations to review their existing approaches to internal and external cyber security. The recent examples of policy reviews indicate a shift of national policy towards cooperative, internationally coordinated and layered approach to cyber security.[5]

In this paper, cyber security will be regarded as a domain addressing security aspects of both information assurance and cyber defense, the latter focusing on

2 The authors wish to express their gratitude to the participants of the 2nd International Cyber Conflict Expert Workshop hosted by George Mason University Center for Infrastructure Protection (GMU CIP) and Cooperative Cyber Defence Centre of Excellence (CCD COE) in April 2009 for discussing and giving valuable feedback on Prof. Wingfield's original concept of the constructs proposed in this article.

3 Prof. Thomas Wingfield is an Associate Professor at U.S. Army Command and General Staff College teaching graduate-level classes in Operational Law, National Security Strategy, and Joint Operations to field grade officers in U.S. Army.

4 Ms. Eneken Tikk is a Scientist and the Head of the Legal Team of the NATO-accredited Cooperative Cyber Defence Centre of Excellence. She was a Research Fellow of GMU CIP and is a PhD student of Tartu University Faculty of Law.

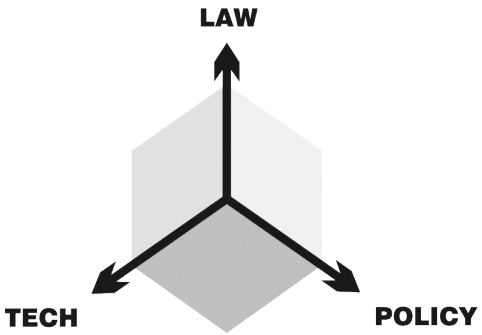
5 Estonia, after suffering politically motivated cyber attacks in early 2007 and triggering the cyber defense policy considerations by NATO, adopted a new cyber security strategy in 2008. The new administration of the US published a consolidated cyber security policy document in June 2009. Both instruments indicate the need for better international coordination and cooperation in cyber incident management.

military/national security approaches to cyber security. Besides the national security aspect, it comprises other background systems that deal with the reasons for and consequences or activities of cyber incidents, namely the economic, intelligence and policy domains. When put into a legal context, these domains will be related to different legal disciplines covering proactive and response measures of cyber security on national and international levels.

To avoid a procrustean approach to cyber security, it is critical to formulate a framework that addresses all the relevant complexities, but that also provides a sufficient clarity to allow those charged with defending nations and networks to make lawful, coordinated, proactive decisions. This paper will seek to provide initial thoughts for such a framework by introducing the Cube - the three inseparable axes of contemporary cyber security; the Pyramid - a stratified legal response to cyber security issues, and the Screen - the digital environment of relevant expertise and interaction.

THE CUBE: POSSIBLE, PERMISSIBLE, PREFERABLE

It has been said that politics is the art of the possible, but it would be more correct to say that in nowadays world *technology* is the art of the possible, just as law is the art of the permissible, and policy is the art of the preferable. The Cube is simply a name for the highest-level organization for reflecting these three dimensions. Displayed, such a Cube would have an x-axis for technology (the possible), a y-axis for law (the permissible), and a z-axis for policy (the preferable).



Each of these dimensions would have a richly detailed hierarchy of supporting information. The Policy dimension, for example, could be organized into the

six categories: diplomacy, intelligence, military, political, legal, and economic (DIMPLE).[6] This DIMPLE construct would allow decision makers in any given area to access the body of information from a perspective that includes as much relevant, and as little irrelevant, information as possible. Determining one's interests and the underlying situation on the axes of the cube, it would be easy to assess what, if any, international legal and policy instruments are there that a policy planner needs to take into account when addressing the response to distributed denial of service attacks under national cyber security strategy.

Further, each area could be organized with an accessible vocabulary and familiar taxonomic structure to add detail to the inquiry, taking into account the cyber incident and envisioned responses in question, *e.g.,* one would be able to narrow the query down to what data protection legal instruments and relevant policy developments address the filtering of network data.

It will be difficult to address all national instruments and approaches in an early model of the Cube. Based on the survey of relevant international instruments, the Cube would indicate the gaps and inconsistencies of international law and policies in the field and, when developed further as a concept at the national level, would also serve as a tool for national policy and law makers to support national cyber security concerns with additional instruments where necessary.

Therefore, the Legal dimension of the first model may be subdivided into internationally addressed disciplines (criminal law, law of armed conflict), and concepts (privacy, freedom of information, telecommunication services, etc). On the national level, the Cube could be much more sophisticated, indicating the source (executive regulations, legislative statutes, judicial decisions, constitutional requirements, recognized international standards), discipline (contract, tort, criminal, administrative), and concept (privacy, terrorism, espionage, fiduciary duty, standards of negligence), with as many subcategories as necessary.

The Technology dimension of the Cube will be based on cyber threat assessment and incident experience. It may reflect the thinking of experts such as Chris Scott of MIT Lincoln Laboratory. Scott organizes technological "attack space components" into attack vectors (user space, kernel, and other), adversary objective (reconnaissance, exfiltration, disinformation, and denial), and attack classes (inject,

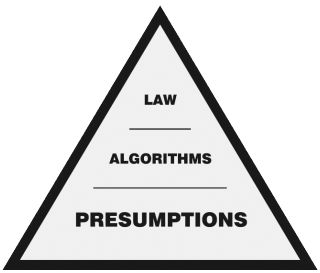
6 The DIMPLE standard proposed by Prof. Thomas Wingfield suggests that since cyber incident reporting requires the use of technical details, the events need to be described in a manner allowing experts of other relevant fields (Diplomacy, Intelligence, Military, Policy, Law, Economy) to understand the report. This promotes expert discussions in the field and avoids parallel vocabulary on topics of common concern.

byzantine, and life cycle).[7] Another way of subdividing the Technology axis would be to look at the types of cyber incidents of security concern for different nations and international organizations, the proposed proactive and defensive measures (*e.g.*, filtering) and the relevant response levels (*i.e.*, the measures that can be taken at the end-user, organization, ISPs, or national government level, as well as the international engagement necessary).

The very complexity of different options, and the multiplicity of possible organizational schemes, argues for a clear meta-structure such as the Technology/ Law/ Policy Cube.

THE PYRAMID

The Pyramid is a conceptual structure which allows us to organize the process of cyber security implementation as opposed to the substance of cyber security. The three layers (Presumption, Algorithm, and Law) reflect the requirement for three levels of decision-making in dealing with cyber security threats, driven by the speed of operations in cyberspace.



The foundational level, Presumptions, are the black-or-white rules built into a system - an instantaneous if-then decision based on objective criteria and requiring no iterative interaction with the threat. Examples would include automatically disconnecting from a server upon receipt of known malicious code, or fencing a user request from a known hostile source. Presumptions must be drawn very narrowly, in that they will be applied without further reflection or authorization by an automated system. The benefit of presumptions is decision-making and reaction in a matter of milliseconds. It is the equivalent of directing sentries

7 Chris Scott, *Cyber Warfare: A perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace,* presented at US Army Cyber Symposium, September 2008.

armed with nonlethal weapons to "shoot" anyone who comes across wire of their military base near enemy territory, and pursue identification and notification only after the immediate threat has been neutralized. To be lawful and prudent, such presumptions must be applicable to any reasonably foreseeable threat upon which they may have to act. Perhaps the clearest application for presumptions would be as the lawful - and necessary - first line of defense for SCADA systems, whose compromise could threaten the lives of thousands. Gradually, presumptions may also refer to righteous expectations towards managing cyber incidents, such as proper quality and availability of log files to be applied by all ISPs.

The intermediate level, Algorithms, is also carried out by an automated system, but it involves a logic tree to authorize further defensive action. The requirement for additional information will drive an iterative process by which the system will quickly gather the minimum data needed to satisfy cyber "use of force" criteria at cyber speeds. These algorithms are more sophisticated than simple "shoot/don't shoot" criteria, but may still be satisfied by a system quickly enough to react to a potentially crippling attack in time to avert serious damage. To continue our real-world analogy, this would be similar to a sergeant of the guard being told to query potential intruders for a recognition signal before ordering his men to open fire. Computers could be 'instructed' to detect potentially malicious activities and engage additional control towards such signals.

The highest level of the Pyramid, Law, is the most nuanced and the least timely. At this level, humans must enter the decision-making process to make high-stakes decisions based on ambiguous or even contradictory information. There is a requirement for the personal accountability of a human "in the loop," and that person must have the benefit of traditional legal counsel. In these cases, a response would take at least minutes, and probably hours. The benefit is the quality of the final product; the cost is the delay in response that could move a cyber operation from immediate defense to one with sufficient deliberation and planning to appear more offensive in nature. Concluding our real-world analogy, this would be the equivalent of a base commander taking several hours to consult with his legal advisor to determine the appropriate range of responses to civilian protesters threatening to breach the base perimeter and put his soldiers and mission at risk. The broader implications of such a decision would require consultation with higher echelons, and would almost certainly include a political judgment to temper the purely legal range of options.

To secure the responsiveness of the Law level of the Pyramid, clear and accurate legal analysis will be critical. The measures to avoid or manage a cyber incident will ultimately have to be supported by appropriate legal determinations, but these

provisions may not always be explicit and easy-to-understand for decision-makers. Therefore, analysis conducted by legal experts will have to take into account the real-life needs indicated by information assurance and cyber defense management authorities and result in conclusions that help other subject area experts apply them in future incidents.

The Pyramid can be constructed upside-down in the sense that the analysis of existing international legal instruments will indicate standards that are most likely applicable in all jurisdictions. Where international instruments are not directly on point, the Algorithms and Presumptions could be based on legal risk analysis, taking into account national best practices and internationally recognized patterns of managing cross-border cyber incidents. However, it bears repeating that since Presumptions are intended to operate automatically and with no immediate human oversight, they must reflect unambiguous determinations of lawful conduct for defense against almost any potential intruder. The challenge will be to maximize available options at all three levels, automating as much of the process as legal precedent, technological savvy and political practicality will permit.

THE SCREEN

The Screen is the final tool we will examine. Whatever theoretical constructs we adopt, and however they are put into practice, they must be put into a form that is quickly and easily accessible to humans engaged in cyber incident management. The Screen is simply the placeholder term for the graphic user interface that will display status and trends, threats and options, probabilities and information gaps.

Much has been learned in the last ten years about presenting high-density information to task-loaded individuals operating under severe time constraints: "all-glass" cockpits in high-performance aircraft, next-generation military command posts, international business networks dependant on highlighting critical data against a high level of background "noise," and even set design for films set in a plausible future, will allow the work of "what if" designers to converge with that of "what is" engineers.

Although perfect real-time knowledge of all cyber threats is an impossible goal, it *is* realistic to do much better at providing a richer, better integrated picture of our cyber security to the technologists, attorneys, and political leaders who will have to collaborate to avert the next cyber attack.

One could think of the Screen as a sophisticated and user-oriented information system delivering the content of hundreds of databases in highly interactive, easy-to-grasp and quickly accessible manner. The visible part of it would be a web space

providing well-structured information about the categories represented on the axes of the Cube. It would contain educational materials, lessons learned, and white papers, as well as relevant legal and policy instruments, providing experts and decision-makers with up-to-date and quality instructions on different aspects of cyber security. The Screen could also identify people, organizations, and authorities who could contribute to cyber incident management. As such, the Screen would not only provide a model for decision-making, but also facilitate communication regarding cyber incidents between national governments and subject matter experts.

CONCLUSION

The Cube, the Pyramid, and the Screen represent complementary approaches to clarifying the complexities of international cyber conflict. These tools comprise a system which can be developed incrementally - perhaps initially at the international level. This version could then be made available for comment and elaboration at the national level. With academic and operational feedback, evolving cyber threat assessments and lessons learned from future cyber incidents, the original system could be improved and refined, capturing the complexity and nuance of diverse national approaches.

The three constructs represent the *status quo* of cyber security law and policy, and highlight issues relevant for regulatory and policy authorities at the international, national, and private enterprise levels. Enhanced national models would provide valuable feedback on potential legal issues, responses, and consequences. Over time, these instruments would help clarify gray areas in law and policy as well as identify impractical legal constraints in need of revision on the national or enterprise level.

IP ADDRESSES SUBJECT TO PERSONAL DATA REGULATION

Eneken Tikk[8]

Abstract

The management of cross-border cyber incidents and conflicts requires extensive and detailed information sharing among governmental agencies and the entities responsible for the often privately owned information infrastructure. The data of interest for the investigation and management of cyber incidents comprises of not only details about the course of action and background of the incidents but also real-time reporting on targets and, most importantly, details of the server logs, which make it possible to differentiate the good traffic from the bad, block hostile IP addresses, and trace the origin of the attacks.

The EU legal framework on data privacy is claimed to create obstacles to processing cyber incident data for the purpose of cooperative cyber defence management. This article examines the applicability of the Data Protection Directive to the processing of IP addresses as part of traffic data and offers ways to overcome legal obstacles in exchanging data regarding cyber incidents.

The article concludes that the current interpretation of the Directive by the European Union data protection stakeholders (Article 29 Working Party and Data Protection Superviser) is contradictory and creates confusion on the national implementation level. The article suggests that more clear understanding of the purposes and nature of processing IP addresses is needed in order to reach meaningful argumentation as to whether such processing is subject to the Directive or not.

1. INTRODUCTION

Systematic data protection in Europe dates to the aftermath of the Second World War and arises from the need to face the threat of people being potentially mistreated

8 Ms. Eneken Tikk is a Scientist and the Head of the Legal Team of the NATO-accredited Cooperative Cyber Defence Centre of Excellence. She was a Research Fellow of GMU CIP and is a PhD student of Tartu University Faculty of Law.

based on an abuse/misuse of personal data available to the state.[9] Nowadays, data protection concerns are touching upon almost all areas of regulation and the recent expansion of cyber threats underlines further the significance of data protection in the context of cyber security as well as cyber incident management. Furthermore, the growing amount of cyber incidents indicate the urgent need to review the data protection framework in order to fight against the growing risk of database infiltrations and loss of sensitive information. Additionally, several groups of stakeholders such as government, industry and individuals are concerned with the topic of data protection while the information technology understanding of data may often differ from the meaning and value of data for marketing and e-commerce perspective where profiling is primarily aimed at satisfying the customer and therefore is very much identity-focused.

As network security has grown from everyone's business into a global concern, and thus requires significant coordination and consultation efforts as a prerequisite of success, the topics of data exchange and data protection are becoming prevalent in policy and legal discussions. In comparison to the first wave of cyber crime regulation in late 90-ies that was driven primarily by commercial interests and resulted in the "mild" law enforcement approach, recent developments in the European Union (EU) legal framework such as the Data Retention Directive and the proposal for the Directive on Attacks Against Information Systems point to a more regulated approach.

Increasing security threats are bound to bring along privacy concerns as solving and investigating cyber incidents may potentially involve processing large quantities of data. Following the latest advancement in the "security vs privacy"

9 In 1939, the German authorities conducted a census to register German Jews and those who were half Jewish with the *Reichssicherheitshauptamt*. While the authorities claimed that personal data, such as religious inclination and nationality, were confidential, a national registry was created on the basis of those data to point out which citizens had a Jewish parent or grandparent. Similar registries were created and updated in Poland and compared to the data of the 1933 census. After the census, the German citizens were listed in the *Reichskartei* as Aryans or non-Aryans and their fate for the purposes of the Second World War was determined by the Nazi authorities controlling those registries. In this context, the statistical data was put to the service of the governing regime. Extremely high regard to population policy transformed normally quantitative data about people into a qualitative and psychological basis of reigning. Although statistical in nature, this information relied on the penetration of private and public lives, recording and categorising such data, and last but not least, subdivision of the data. The census data based on religion and nationality were not the only listed categories of information. In 1935, the authorities created the labour registry, in 1936 the health registry, in 1939 the population registry, and in 1944 the personal identification number system. From 1934 on, those with hereditary illnesses were registered. By the beginning of the war, the authorities had a clear picture of family planning, land inheritance and health status of the population. These statistics were put to service by and under the control of the authorities. Summarized from „The Nazi Census: Identification and Control in the Third Reich (Politics, History, and Social Change)" by Gotz Aly, Karl Heinz Roth, Edwin Black, and Assenka Oksiloff, Temple University Press, 2004.

polemic, the application of data protection rules in responding to cyber incidents needs even further attention from IT security stakeholders since IP addresses and other network traffic data that is daily exchanged between trusted parties around the world may be viewed as personal data and consequently, their processing may be rendered legally problematic.

This article uncovers some of the most challenging issues in the debate on whether IP addresses should be considered as personal data and thereby subject to the EU Data Protection Directive 95/46/EC[10]. Moreover, it needs to be analysed to what extent other EU legal instruments apply to the regulation of IP addresses and what is the Working Party 29 (WP 29) position in the slightly controversial matter.

2. THE PROBLEM AROUND THE INTERPRETATION OF THE DATA PROTECTION DIRECTIVE 95/46/EC

Essentially, the EU data protection regulatory framework is based on the prohibition of processing personal data and has issued different exceptions that allow the data to be processed under a set of personal data protection principles and restrictions.

Directive 95/46/EC has become the cornerstone of data protection in Europe and serves as the basis and a role model for personal data protection legal acts in more than 30 advanced information societies worldwide. Currently, personal data can be freely exchanged and processed between the 27 EU member states and three European Economic Area (EEA) member countries (Norway, Liechtenstein and Iceland) and to Switzerland, Canada, Argentina, Guernsey, and the Isle of Man. Transfer of personal data to the third countries is only allowed if the third country in question ensures an adequate level of protection.[11] An exception to that principle is granted to the US Department of Commerce under the Safe Harbour Framework[12], and the transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection[13]. Not surprisingly, one of the most critical problems includes the legal difficulties in exchanging data between nations, authorities, industry and other stakeholders.

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, available online at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

11 Data Protection Directive 95/46/EC, Chapter IV, Transfer of data to third countries.

12 *US-EU & Swiss Safe Harbor Frameworks, available online at: http://www.export.gov/safeharbor/.*

13 Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security, DHS, 2007 PNR Agreement.

In the context of sharing cyber incident data, one possible interpretation of the Directive leads to the conclusion that collecting and exchanging IP addresses is subject to the conditions provided for in the Directive. The other leaves IP addresses out of the immediate scope of the applicability and requires the Directive to be followed only in case the use of IP addresses would identify the person behind it. Hence, the essence of the problem lies in determining the scope and ability of IP addresses to perform as individual identifiers as well as the applicability of the EU Data Protection Directive.

The first elements of the puzzle are inevitably the definitions of "IP addresses" and "personal data". Electronic Privacy Information Centre's (EPIC) approach to describing an IP address as part of traffic data is generally widely supported:

> "A device's (typically a computer's) numerical address as expressed in the format specified in the Internet Protocol. In IPv4, the current addressing format, an IP address is a 32-bit sequence divided into four groups of decimal numbers separated by periods. In some circumstances, the IP address identifies a unique computer. In other circumstances, such as when a network of computers connects to the Internet via a single Internet connection, it may not. An IP address for a computer is similar to a telephone number for a telephone."[14]

As the foundation for the forthcoming discussion the article employs the terminology of the EU Data Protection Directive whilst it is useful to note that not everyone involved in the debate is proficient in and uses the terminology of the Directive. When engaging in discussions with the US legal communities, the term "personally identifiable information" (PII) comes up, which essentially is a synonym to "personal data" as defined in the Directive.

The Directive defines as personal data and therefore as potentially applicable to processing "any information relating to an identified or identifiable natural person ("data subject")".[15] An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[16].

Further, the word "indirectly" plays an important role in how this definition is understood in the context of IP addresses. The Directive itself provides no further definition for this term, but it has been addressed by Article 29 Working Party[17] set up under Article 29 of the Data Protection Directive.

14 Definition of an IP address, Electronic Privacy Information Centre, available at: http://www.epic.org.
15 Article 2 (a) of the Directive.
16 Article 2 (a) of the Directive.
17 WP 29 is an independent European advisory body on data protection and privacy having great influence on national interpretation of the Directive.

According to WP 29, as regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others.[18]

Although not the core of this debate, another important term is "processing" that for the purposes of the applicability of the Directive means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[19] Thus, if concluded that IP addresses are personal data, the Directive is applicable to all possible occasions of processing.

Therefore it is of utmost importance to reach a conclusion whether IP addresses should be considered as personal data. Should that be the case, several entities such as Internet Service Providers (ISPs), search engines, etc would be subject to a number of obligations stated in the Directive. For example, the data controller (the entity processing data) is responsible for ensuring that data be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, accurate and up to date as well as kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[20] Most importantly, the controller is obliged to provide information about the fact of the processing as well as the existing data to the data subject.[21]

3. APPLICABILITY OF THE DATA PROTECTION DIRECTIVE TO THE PROCESSING OF IP ADDRESSES: VIEWS AND REASONING

Needless to say, there are several contradicting opinions about the applicability of

18 Opinion 4/2007 on the concept of personal data (WP 136). Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.
19 Article 2 (b) of the Data Protection Directive.
20 Data Protection Directive 95/46/EC, Article 6.
21 Data Protection Directive 95/46/EC, Article 6.

the Directive.[22] The views on the debate concerning IP addresses that have been echoed by the EU Data Protection Supervisor (EDPS), Working Party 29 and several data commissioners[23] are rather conservative, in most cases regarding IP addresses and traffic data as personal. This chapter will look into the recent policy discussions in the EU, opinions of Article 29 Working Party (hereinafter WP 29), an independent EU Advisory Body on Data Protection and Privacy established by Article 29 of the Data Protection Directive, and introduce two further directives impacting the processing of IP addresses.

3.1 Position of the European Union Data Protection Supervisor

According to the European Union Data Protection Supervisor (EDPS) Peter Hustinx, a person does not have to be identifiable by name for data protection law to apply to details of their computer usage. Hustinx stated that companies, if in doubt, should treat all user activity, server logs and records of IP addresses as personal data. The Data Protection Supervisor further claimed that in order for an IP address to count as personal data there is no requirement for the company processing the data to know details such as the name, birth date or other personal data of the individual whose activity it was monitoring. Rather individuals are identifiable when they are singled out and, according to Hustinx, tracking the behaviour of individuals by their IP address singles individuals out in such a way as to make them identifiable.[24]

In a recent opinion on the current negotiations by the European Union on the Anti-Counterfeiting Trade Agreement (ACTA) the EDPS[25] has once again underlined the importance of the regulation of personal data processing. Even though the opinion is determined to focus on intellectual property infringement, it clearly scrutinises the relationship between IP addresses and personal data.

In the above-mentioned opinion the EDPS notes that Directive 95/46/EC is applicable to the processing of IP addresses involved in the three strikes Internet disconnection policies where the IP addresses "should be considered as personal

22 Article 29 WP Asks More Data Protection From Search Engine Operators, Digital Civil Rights in Europe, available at: http://www.edri.org/edrigram/number8.11/article-29-wp-search-engines; Working Party 29 Chairman Jacob Kohnstamm's letter to Google, 26 May 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf.

23 Aoife White, IP Addresses Are Personal Data, E.U. Regulator Says January 22, 2008, available at http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html.

24 *Via McCann FitzGerald Solicitors;* ZDNet interview with Peter Hustinx, available at: http://news.zdnet.co.uk/security/0,1000000189,39540137,00.htm.

25 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010/C 147/01, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf.

data. IP addresses are identifiers which look like a string of numbers separated by dots, such as 122.41.123.45. A subscription to an Internet access provider will give the subscriber access to the Internet. Every time the subscriber wishes to go onto the Internet, he will be attributed an IP address through the device he is using to access the Internet (a computer, for example)".[26] Hereby EDPS confirms its earlier position that IP addresses should be viewed as personal data.

EDPS continues that "the principles of protection must apply to any information concerning an identified or identifiable person" and confirms that if a user engages in a given activity, for example, uploads material onto the Internet, the user may be identified by third parties through the IP address he/she used.[27] Therefore, for the purposes of ACTA:

> "Traffic data such as IP addresses may only be collected and stored for reasons directly related to the communication itself, including billing, traffic management and fraud prevention purposes. Afterwards, the data must be erased. This is without prejudice to the obligations under the Data Retention Directive which, as discussed, requires the conservation of traffic data and its release to police and prosecutors to aid in the investigation of a serious crime only. This means that, when contacted by copyright holders, unless such contact occurred within the limited period outlined above, ISPs should not have the log files linking the IP addresses to the relevant subscribers. Retaining the log files beyond such period should only be done for justified reasons within the scope of the purposes provided by law."[28]

3.2 WP 29 opinions regarding IP addresses as personal data

WP 29 opinions are authoritative for the national implementation of the Directive as the body is composed of heads and high-level representatives of national data protection agencies. The advisory body has issued a number of opinions where the topic of IP addresses has been addressed. As will be shown below, the opinions leave very little opportunity for monitoring traffic without being obliged to implement data protection requirements.

WP 29 shares EDPS's perspective on the processing of personal data. WP 29's argumentation in this opinion is reflected already in 2000, where WP 29 considered IP addresses as data relating to an identifiable person. It has stated that "Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally

26 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), p. 25.
27 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), p. 26.
28 Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), p. 57-59.

systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive …)."[29]

In its 2008 opinion on search engines, WP 29 observed:

> "A search engine provider that processes user data including IP addresses and/or persistent cookies containing a unique identifier falls within the material scope of the definition of the controller, since he effectively determines the purposes and means of the processing."[30]

WP 29 further explained that in the role as service providers to the users, search engines are collecting and processing vast amounts of user data, including data gathered by technical means, such as cookies.[31] A search engine provider may link different requests and search sessions originating from a single IP address[32]. It is thus possible to track and correlate all the web searches originating from a single IP address, if these searches are logged. Identification can be improved, when the IP address is correlated with a user unique ID cookie distributed by the search engine provider, since this cookie will not change when the IP address is modified.[33] In the context of this article the term "search engine provider" could be compared to an Internet Service Provider.

But even if we were talking about entities monitoring traffic for their own "internal" purposes the opinion of WP 29 would still render them subject to data processing regulation. WP 29's further reasoning concludes that though IP addresses are in most cases not directly identifiable by search engines, identification can be achieved by a third party. Law enforcement and national security authorities can gain access to such data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.[34]

To further explain the effect of this interpretation, these conclusions have impact

29 WP 29 Working Document "Privacy on the Internet - An integrated EU Approach to On-line Data Protection. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.
30 WP 29 opinion on data protection issues related to search engines, 4 April 2008, available at: http://www.registratiekamer.nl/downloads_int/c.1.a_ts_search_engines_adopted_version.pdf.
31 Opinion 1/2008 page 4.
32 An increasing number of ISPs distribute fixed IP addresses to individual users.
33 Opinion 1/2008 page 7.
34 Opinion 1/2008 page 8.

also beyond the EU. According to the SWIFT Opinion from 2006[35] a data controller may effectively be an entity not located on the territory of any EU Member States.

All in all, these arguments create an intriguing "data protection limbo", where data is regarded personal, because it can potentially be accessed by law enforcement and national security agencies, while other directives[36] request the same data to be made available to such authorities.

3.3 Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)

The analysis of the Data Protection Directive is incomplete without regard to the interpretation of Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)[37] adopted in 2002 regulating privacy and personal data protection in the electronic communications sector. This directive introduces the term "traffic data" meaning any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.[38] Although it is important to note that the e-Privacy Directive distinguishes a portion of data for the "communication conveyance" point of view, the aim of the instrument is to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy.[39]

Despite the fact that the Directive does not explicitly address IP addresses, they are still included in the definition of traffic data. The e-Privacy refers to traffic data as a set of data undergoing a different regulatory regime for network conveyance purposes and thereby recognizes to an extent the need to adjust technical and legal notions of data. Yet, the Directive seeks to find a balance and thus stresses that privacy rights remain the primary concern for communication service providers when processing traffic data.

Valuable insights to the current interpretation of the extent of the applicability of the Data Protection Directive to data processing for information security purposes

35 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.
36 E.g. Data Retention Directive.
37 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal L 201, 31/07/2002 P. 0037 – 0047. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.
38 Article 2 (b) of the e-Privacy Directive.
39 Article 1 (a) of the e-Privacy Directive.

are provided by WP 29 in an opinion regarding the proposed amendment[40] of the e-Privacy Directive in 2009.[41]

According to the proposed amendments, the public communications providers are obliged to to inform national regulatory authorities of any data security breach. In the process of discussing the amendments, the Parliament proposed to introduce a new Recital (27a) on IP addresses in the e-Privacy Directive.[42] The proposal reads as follows:

"IP addresses are essential to the working of the internet. They are unique numbers assigned to devices participating in a computer network using the Internet Protocol for communication between its nodes, such as computers or mobile smart phones. In practice, they may also be used to identify the user of a given device. Considering the different scenarios in which IP addresses are used, and the related technologies, which are rapidly evolving (including the deployment of IPv6), questions have arisen about their treatment as personal data in certain circumstances. Developments concerning the use of IP addresses should be followed closely, taking into consideration the work already done by, among others, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC, and in the light of such proposals as may be appropriate."[43]

The response of the WP 29 to this proposal allows concluding that it considers the issue of IP addresses having been addressed and solved with sufficient clarity:

> "The Working Party does not support the proposal to make an explicit reference to this issue in a directive. In this respect, it re-emphasizes its earlier Opinion[44] that unless the service provider "is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as

40 New e-Privacy Directive 2009/136/EC that is amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

41 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf.

42 COM (2008) 723 (Amended proposal for Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation (EC) No 2006/2004 on consumer protection cooperation (Text with EEA relevance), page 21 (amendment 185). Available online at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0723:FIN:EN:PDF.

43 COM (2008) 723, page 21.

44 Opinion 4/2007 on the concept of personal data and Opinion 1/2008 on data protection issues related to search engines.

personal data, to be on the safe side".

In the above mentioned opinion the Article 29 Data Protection Working Party concludes that unless the service provider "is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side". IP addresses relate to identifiable persons in most cases. Identifiability means identifiable by the access provider or by other means, with the help of additional identifiers such as cookies or in interactions with internet services with which the data subject is identified explicitly or implicitly.[45]

WP 29 underlines that a substantive provision of a directive is not the most suitable way of addressing this issue and that a reporting obligation referring to "purposes not covered by this Directive" is not appropriate.[46] This remark by the WP 29 puts special emphasis on the service provider's ability to distinguish between the data that can be linked with a certain identity and the data that cannot be identified.

In sum the Working Party has rejected the need to amend the Directive in order to allow processing IP addresses as it sees that this option already exists under the current wording of the Directive. Considering, however, the opinions given under the Personal Data Protection Directive, the two views are opposing. To illustrate this conflict, the Data Retention Directive needs to be looked into.

3.4 Data Retention Directive 2006/24/EC

The Data Retention Directive[47] creates the "missing" link between the data in the communication service provider's possession and the potential processing for law enforcement purposes.

The purpose of the Data Retention Directive is to harmonize Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communication networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data is available for the purpose of the investigation,

45 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf.

46 *Ibid.*

47 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Official Journal L 105, 13/04/2006 P. 0054 – 0063. Available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML.

detection and prosecution of serious crime, as defined by each Member State in its national law.[48]

For the purposes of the Data Retention Directive, data means traffic data, location data and the related data necessary to identify the subscriber or the user.[49] IP addresses are data needed to identify a particular user and fall under the categories of data that need to be retained according to Article 5 of the Directive. The data should be retained to the extent that it is generated or processed by providers of publicly available electronic communication services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.[50]

It therefore provides the ground for data exchange between communication service providers and law enforcement. Although defining the exact scope of law enforcement authority is left to national law, the wording of the WP 29 in its Opinion 1/2008 leaves little room for alternative interpretation: if it is likely that the data retained by the communication service providers is available to national authorities upon request, the data is to be regarded as potentially identifying a data subject[51].

4. SUMMARY AND THE NEED FOR FURTHER CLARIFICATION

If we combine the requirements set in the directives with the opinions of the WP 29 and EDPS, we reach a situation where the notion of personal data and therefore the legal implications put forward in the Data Protection Directive are applicable to a very broad range of information. In keeping with these arguments, it appears that the sole option for processing traffic data, including the IP addresses, without falling under the scope of the Data Protection Directive would be during real-time monitoring when no data is stored for further analysis (and availability).

The issue of IP addresses as personal data has also been looked into on the national level. The outcome indicates that countries have taken different positions as regards the implementation of the Directive, which, in the longer run could lead to additional policy concerns in the EU. Positions of national authorities in Germany, France, UK and Sweden illustrate the wide spectrum of approaches[52] where it

48 Article 1 of the Data retention Directive.
49 Article 2 (a) of the Data Retention Directive.
50 Article 3 (1) of the Data Retention Directive.
51 Opinion 1/2008 page 8.
52 The developments in these countries have been covered in more detail in: Tikk, Eneken, Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective. In NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Volume 59, 2009 „Modelling Cyber Security: Approaches, Methodology, Strategies", pages 189 - 198.

becomes evident that, for example, depending on the national regulation and court's interpretation, the dynamic IP addresses may be considered as personal data[53] or as not personal data.[54]

Seen from the EU perspective, difference in opinions poses a threat to the uniform application of the directives and in the broader perspective to the value and position of the EU law in general.

5. RECOMMENDATIONS FOR NATIONAL IMPLEMENTATION

5.1 National Security Exceptions

The applicability of the Directive is bound to its scope. In accordance with Article 3(2) of the Data Protection Directive it shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law /…/ and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

Similarly, Article 15(1) of E-Privacy Directive sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in this Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications systems.

Another perspective that will potentially play a role in the debate around the applicability of the Directive to processing traffic data is processing network monitoring information for law enforcement and national security purposes.[55]

53 District and Regional Court of Berlin, 2006, see more Lundevall-Unger, Patrick, Tranvik, Tommy, IP Addresses – Just a Number?, International Journal of Law and Information Technology, University Press 2010.

54 District court of Munich, 2008, see more Lundevall-Unger, Patrick, Tranvik, Tommy, IP Addresses – Just a Number?, International Journal of Law and Information Technology, University Press 2010.

55 WP 29 has observed that: „Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address. (Opinion 1/2008 on search engines).

Nations could make use of the national security exception of the Data Protection Directive. The general national security exception should also be included in other legislative instruments, primarily in relation to the authorities and procedures involved.

5.2 Complying with WP29 Opinions

WP 29 has concluded that as long as the service provider in the capacity of data controller is able to distinguish that network traffic data is not personally identifiable, such data is not regarded personal in the context of the EU Data Protection Directive. It would be safe to conclude that real-time monitoring with no data retention would be in compliance with the current regulatory framework of the EU.

Until no further guidance is provided, these are the steps that could be taken by communication providers and national legislative authorities to reduce the risk of processing IP addresses in violation of the Data Protection Directive.

5.3 Following up the discussions on national level

National data protection authorities could serve as the balancing power between cyber security concerns and privacy rights. A balanced guidance on network monitoring would assist communication providers who eventually need to assess the need for network monitoring and make sure that all data processed is proportionate with the actual security assessment and that data is retained for no longer than necessary.

WP 29 concludes that the legislative measures limiting the right to privacy of individuals have to be accessible and foreseeable as regards their implications for the persons concerned.[56] This principle requires the legislation to be sufficiently clear in its definitions of the circumstances, the scope and the modalities of the exercise of interference measures. The provisions have to be unambiguous and go into detail to indicate under which circumstances the public authority authorized to take measures limiting fundamental rights. They should in particular specify where such measures may be used and should exclude all general or exploratory surveillance and offer protection against arbitrary attacks from public authorities.[57]

56 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf.
57 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. Available online at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf.

My personal position is that the decisive factor should not be the nature of IP addresses as such, but the purpose of processing - i.e. IP addresses can be personal data when used in investigation, but for the purpose of managing the networks and possibly also monitoring traffic and exchanging information about anomalies, the important factor is that the purpose of such processing is not to identify the individual (which is the core concern of the Directive) but detecting threats, vulnerabilities and potential defences.

Therefore, for the purposes of law enforcement and also in cases where one would use IP-addresses and other traffic data to identify the person behind an intrusion such data processing is subject to the Directive, but all uses of the same data for network management purposes is not.

5.4 Additional clarification by WP29

So far WP29 has rejected the proposal to clarify the legal framework of processing IP addresses (see section 3.3. "Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)").

Considering the opinions of WP 29 in assembly, an indubious position cannot be derived. It would be therefore rational for the WP 29 to expressly address the issue of processing IP addresses and/or traffic data for the purposes of network security and global cyber security concerns.

Thereby WP 29 would not only respond to an important concern shared by many nations but also eliminate part of the margin of interpretation potentially undermining the value and weight of the EU data protection directives. The guidance given by WP 29 would significantly aid to more coherent implementation of the legal framework of personal data processing by Internet Service Providers, Critical Information Infrastructure entities, law enforcement and those facing cyber attacks as part of their cyber threat assessment.

CONCLUSION

There is no doubt about the interrelation of data protection and cyber security. However, the current definition of personal data appears to restrict monitoring of traffic and detecting anomalies. In addition to the debates in legal and technical communities, the issue of IP addresses has been discussed by a number of national authorities and the results of these discussions reflect a divide of implementation practices. WP 29 has concluded that as long as the service provider in the capacity of data controller is able to distinguish that network traffic data is not personally

identifiable, such data is not regarded personal in the context of the EU Data Protection Directive, but WP 29-s other opinions restrict this position and lead to the conclusion that only real-time monitoring with not data retention is legally feasible. This does not, in many cases, satisfy the needs and requirements of technical experts.

To resolve the issue, difference should be made between processing data for mere monitoring, and processing data in order to identify the IP address user. Also, nations need to make better practical use of the national security exceptions under the Data Protection and E-Privacy Directives.

In sum, a more nuanced approach is needed to whether and under what circumstances IP addresses and other traffic data are to be processed in full compliance with the personal data protection requirements. Also, it should be considered if there are options for partial applicability of the Directives. For a better way ahead, national practices of implementing the Directive need to be studied and analyzed.

DEVELOPMENTS IN THE LEGISLATIVE, POLICY AND ORGANISATIONAL LANDSCAPES IN ESTONIA SINCE 2007

Kadri Kaska[58], Anna-Maria Talihärm[59], Eneken Tikk[60]

Abstract

In April and May 2007, Estonia faced coordinated cyber attacks targeted at the Estonian governmental and commercial entities. The attacks drew strong attention to the need to raise international awareness about politically motivated and coordinated cyber attacks directed against a nation state and, more generally, against the modern information societies that are increasingly dependent on information technology. Three years after the attacks, it is increasingly evident that cross-border cyber incidents such as Estonia 2007 touch upon legal norms of different legal fields and therefore need to be viewed from the three-fold prism of Law of Armed Conflict, Criminal Law, and IT legal framework, thus supporting the comprehensive approach to the domain. This article examines the developments in the area of cyber security in Estonia and in what ways the Estonian legislation, policy approaches as well as organisational landscape have evolved since April 2007.

INTRODUCTION

The level of dependency on information technology and differences in approaches, in motivation of interest groups as well as principles employed in regulating information societies vary greatly from nation to nation. This combined with the rapid progress of information technology often complicates the practical implementation of legislative measures necessary to ensure cyber security at the national and, moreover, at the international level.

58 Kadri Kaska is a Junior Scientist of the NATO-accredited Cooperative Cyber Defence Centre of Excellence.
59 Anna-Maria Talihärm is a Junior Scientist of the NATO-accredited Cooperative Cyber Defence Centre of Excellence and a PhD student of Tartu University Faculty of Law.
60 Eneken Tikk is a Scientist and the Head of the Legal Team of the NATO-accredited Cooperative Cyber Defence Centre of Excellence. She was a Research Fellow of GMU CIP and is a PhD student of Tartu University Faculty of Law.

Similarly, the expanding divide between the views of legal scholars in the field of cyber defence law produces numerous valuable theories, doctrines and guidance without having too much regard to counterarguments and assessments of the practical impact from policy and technological perspective. This, in return, brings about the unfortunate effect of a colourful abundance of articles, books, conferences on the subject and a number of think tanks dealing with cyber issues, while at the same time players involved in real-life cyber incidents have access only to a handful of practical solutions.

Much has been written on the legal aspects of cyber security and defence, and most of these discussions can be divided into three main research areas: Law of Armed Conflict (LOAC), Criminal Law, and practical IT Law. However, much of this research has been stove-piped, i.e. focused on the specific area of expertise and individual security planning instead of a coordinated and interdisciplinary approach.

There are multiple reasons why legal research in the cyber security/defence area has developed in such isolated manner, two of them being the most relevant. First, for a long time cyber defence has been a "closed circuit" responsibility and domain of individual corporations, governments, organisations and working groups. This has led to a situation where numerous think tanks exist in the field but no general agreement seems to prevail that would include practical input for those who have to respond to contemporary cyber incidents.

The second reason – which very much derives from the first one – is that the wide spectrum of cyber threats has not been visible to all subject matter experts at the same time in the same manner. While the military domain has dealt mainly with information operations (IO)[61] and electronic warfare (EW)[62], criminal law experts have been busy with identity theft and credit card fraud[63], and IT legal experts have been working on developing legal policies that would harmonise the security concerns of the private sector with public and national interests[64].

In this context it is understandable how various players such as nations and organisations have ended up with different views on the domain of cyber security. Different perspectives, however, should not prevent nations from critically reviewing their regulation in the context of new emerging threats and

61 Information Operations, Joint Publication 3-13, Joint Chiefs of Staff, US Army, 2006, available at: http://www.fas.org/irp/doddir/dod/jp3_13.pdf.
62 Electronic Warfare, Joint Publication 3-13.1, Joint Chiefs of Staff, US Army, 2006, available at: http://www.fas.org/irp/doddir/dod/jp3-13-1.pdf.
63 Online Identity Theft, OECD, Directorate for Science, Technology and Industry, 2009, available at: http://www.oecd.org/document/44/0,3343,en_2649_34223_42420716_1_1_1_1,00.html.
64 Strategies for Cybersecurity and Critical Information Infrastructure Protection, ITU, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html.

implementing a comprehensive approach to cyber security by involving a wide range of stakeholders, coordinated decision-making and multiple areas of regulation.

The aim of this article is to follow closely the development of cyber security framework by examining the legal aftermath of the Estonia 2007 cyber attacks. The article argues that a practical and viable approach to cyber security and defence – one that is able to offer a comprehensive set of effective measures for preparedness, response and mitigation – includes all of the above-mentioned fields of law.[65]

Thereby, the article will use the Estonia 2007 case study to demonstrate, with the benefit of a 3-year retrospective, the legal, policy and organisational lessons learned from a cyber incident. Based on the assumption that the changes undergone reflect weaknesses in the legal system identified by the attacks, we may presume that these were the areas of information society regulation where the need for amendments was most clear. The study also suggests that the first steps for a nation that aims for a better coordination in the domain of cyber security would be defining relevant terminology, reviewing the legislative system, and enforcing effective application of the cyber security strategy.

Different Perspectives on Cyber Security

Cyber incidents such as Georgia 2008[66], Lithuania 2008, Radio Free Europe/Radio Liberty 2008 have reinforced the understanding that conflicting points of view often tend to arise from different background systems[67] and experiences that do not support the same or even similar legal conclusions.[68] Consequently, the ability to consider the different relevant sides of the story and the ability to systematically categorise the different types of cyber activities has enormous significance from the legal perspective. Under the rule of law and especially the principle of *nullum*

65 This approach can also be called Frameworks for International Cyber Security (FICS). Read more, Tikk, Eneken, Frameworks for International Cyber Security. CCD COE Publishing, 2010.

66 The Georgian incident especially illustrated the need to look to the criteria of applicability of different legal regimes and the remedies available therein. Both are addressed in Tikk, Eneken; Kaska, Kadri; Vihul, Liis, International Cyber Incidents: Legal Considerations, CCD COE, 2010, See pp. 25-26 for Estonia and pp. 79-88 for Georgia.

67 While international law and law of armed conflict tend to be what many practicing attorneys would call "too abstract for a good argument", IT legal issues are very practical and often do not have a long legal history behind them. It is therefore seldom that lawyers have to practice both of these disciplines.

68 For a more complete fact description and legal analysis, see Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010.

crimen nulla poena sine lege[69] known to criminal law, it may be highly complicated to draw any legal consequences from an act that cannot be clearly related to an existing legal regime or framework. From a practical point of view, therefore, a clear understanding of "what is what" in terms of applying the corresponding legal regime is of crucial importance.[70]

Side by side with the necessity of taking into account the various national approaches to cyber security it is vital to integrate these different perspectives in order to define a common point of departure for managing cyber security incidents. As explained above, a segmented approach often continues to prevail within law related to national cyber security. The historic segmentation of different fields of law has caused employing a similar segmented approach in the domain of cyber security regulation. While there are examples of countries that have adopted or are currently preparing or considering cyber security "umbrella acts"[71] intending to address a number of cyber security related legal issues within one law, it is also true that none of those cases truly involve all areas of law relevant to cyber security. Rather, they are often aimed at achieving particular cyber security objectives, address diverse national cyber security problems, and originate from very different reasons, which is why it is difficult to derive a regulatory model based on these examples.

There are arguments that speak for an all-inclusive cyber security regulation – re-structuring the current system of a number of ministries and public institutions all sharing the competence over cyber security under one overseeing body would better coordinate national initiatives, cut back on duplicated effort and waste of resources, as well as result in a more effective overall defence. However, a comprehensive approach does not necessarily mean that all cyber-related matters of different fields should be brought under a common legal framework and/or a common managing body. In fact, there are sound arguments to indicate that the

69 The principle of '*nullum crimen, nulla poena sine lege*' originates from continental European legal systems and has nowadays become a fundamental right which is enshrined in several national constitutions and a number of international instruments. In Estonian legislation, the principle is stated in the Estonian Penal Code (§ § 2 and 5). The n*ullum crimen, nulla poena sine lege* principle is a legal principle that prohibits retrospective criminalisation of acts and omissions. The principle states that no person may be punished for an act that was not a criminal offence at the time of its commission and results in the prohibition of applying law by analogy and requirement of specification of an offence.

70 The issue of how to categorise information warfare attacks is of more than academic interest. First, whether or not an information warfare attack can be considered an act of "war", "force" or „aggression" is relevant to whether a particular response would be proportionate to the original attack. See Greenberg, Lawrence T. and others, Information Warfare and International Law, 1998, page 19.

71 E.g. the U.S.A. (Protecting Cyberspace as a National Asset Act 2010), India (Information Technology Act 2000), Latvia (Cyber Security Framework Act, draft as of summer 2010), and Slovakia (the drafting of a uniform legal act was discussed in the spring of 2010).

reverse may be advisable.

One of them lies in the evolvement of regulating information technology. Since cyber is not a "thing in itself" but a merely a means to support the functioning of state and society, law of information technology has developed under the same concept of regulation supporting certain societal functions on a sectoral basis. It may be unreasonably resource-consuming, if not entirely unrealistic, to reshape the legal systems from a function-based to a tool-based approach. This function-based approach is also reflected in the current setup of and task division between national administrations, where a balance is needed to ensure that one agenda does not unduly dominate over another, equally justified one (e.g. security over economic growth and welfare or *vice versa*).

However, a comprehensive approach does mean that there should be a greater degree of involvement of different bodies shaping and affecting policy in cyber related matters, and a greater level of cooperation between them, which is where national cyber security strategy drafting might come in as a useful forum.

Overview Of The Estonia 2007 Incident

In the spring of 2007, Estonia suffered from an unprecedented amount of coordinated cyber attacks against its private and public institutions. The attacks – mainly denial of service (DoS) and distributed denial of service (DDoS) attacks – were triggered by the relocation of a Soviet World War II war memorial and targeted at the Estonian governmental agencies, banks, as well as media channels and private web sites. At the their peak, the amount of data traffic originating from the outside of Estonia and targeting governmental institutions was hundreds of times higher than its normal rate.[72] While the intensity of attacks or the choice of targets was not completely unprecedented, the extent, amount and duration of the attacks combined and the manner of coordination employed was not comparable to anything that a single nation state had experienced, and the sequence of attacks quickly gained attention worldwide.

Estonia has over the years become an example of an effective e-state[73] where an impressive choice of public e-services and databases – governmental as well as commercial – has been integrated into a nation-wide information system accessible throughout the country. The high level of IT development reveals an increasing dependence on e-services and the Internet as well as explains the vulnerability of

72 Tikk, Eneken, Oorn, Reet, Legal and Policy Evaluation: International Coordination of Prosecution of Cyber Terrorism, 2007.

73 A few examples: Estonia was the first country to hold Parliamentary elections online in 2005 and 95% of Estonia's banking operations are carried out electronically.

the country to a wide range of cyber offences. This dependency and vulnerability is characteristic to all modern information societies.

The attacks started on April 27 and disrupted Estonian e-services and information infrastructure in several waves of varying intensity until the end of May. Roughly, two phases could be distinguished in the incident: an initial emotional cyber response to the government's political decision of relocation of the monument (which ran in parallel to riots on the streets of the country's capital) was soon followed by more sophisticated and coordinated cyber assaults. The first phase lasted for a few days and was characterised by relatively simple DoS attacks against government web servers and Estonian news portals. The attacks did not appear to be centrally coordinated and were carried out mostly on *ad hoc* basis, boosted by online step-by-step instructions with a pre-defined list of targets.[74]

The second phase was characterised by the use of larger botnets and more sophistication[75] with the attacks involving more than 85,000 hijacked computers.[76] The abrupt waves of attacks[77] referred to better coordination; also a clear correlation was noticeable between the politically significant dates and intensification of the attacks.[78] Similarly to the first phase, Internet forums and chat rooms were used to distribute instructions and information about launching the "do-it-yourself" attacks but most of the attacks launched during the second phase appeared to be better and more systematically coordinated.

Some of the DDoS attacks were temporarily successful and managed to disable the online services of two biggest banks in Estonia and at one point shut down 58 websites[79] at the same time. Additionally, various attacks were performed against critical routers at Internet service provider level, which disrupted the government's Internet based communication for a short period of time. On top of that, both of the phases included website defacement and large amounts of email and comment spam.

Even though from a conservative lawyer's point of view, the Estonian 2007 cyber attacks did not amount to more than a series of cyber crimes, the media quickly

74 Evron, Gadi, Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War, Georgetown Journal of International Affairs, Winter/Spring 2008, p 121-126.
75 Nazario, Jose. Estonian DDoS Attacks - A summary to date, 17.05.2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.
76 Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010, p. 20.
77 Graphs about the Estonian cyber attacks 2007, available at: http://www.riso.ee/wiki/Riots.
78 Tikk, Kaska, Vihul, Legal Considerations, p 18.
79 Nazario, Jose. Estonian DDoS Attacks - A summary to date, 17.05.2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

labelled the attacks "Cyber War I".[80] Security analysts argued that in comparison to other DoS and DDoS attacks[81], the size of the Estonian attacks was not groundbreaking.[82] Similarly, the Estonian government concluded in June 2007 that the cyber-attacks carried out against Estonia in April and May did not paralyse the country's normal daily activities, although, under certain conditions, could have posed a significant security risk.[83] On the international level, it was the element of political and social motivation that rendered the attacks globally noteworthy.

Since attribution is one of the crucial elements in solving any cyber incident, the identification of the attacker received significant attention both on national and international communities. There still prevails a popular belief that the large-scale cyber attacks against the Estonian government's servers and critical private information infrastructure in 2007 were initiated by and carried out from Russia. However, Konstantin Goloskokov, a member of a pro-Kremlin youth association *Nashi*, has been so far the only person publically admitting[84] taking part of the cyber attacks stating that "cyber attacks against Estonia seemed to be the only possible step."[85] Despite speculations on the political level[86], the exact origin of the attacks has not been confirmed in legally waterproof terms. What can be deducted from available facts is that a part of the attacks was carried out voluntarily by regular citizens and Internet users following instructions and sharing experiences on web forums (albeit mostly Russian)[87], and that the attacks were dispersed worldwide involving computers from 178 countries[88]. Nonetheless, any government's explicit role in the attacks cannot be confirmed.

Technical Measures Of Response

In the 2007 cyber attacks, the Computer Emergency Response Team of Estonia

80 Landler, Mark; Markoff, John. 'In Estonia, what may be the first war in cyberspace.' International Herald Tribune. 28 May 2007. http://www.iht.com/articles/2007/05/28/business/cyberwar.php.
81 Vamosi, Robert, Cyberattack in Estonia--what it really means, ZDNet, available at: http://www.zdnet.com/news/cyberattack-in-estonia-what-it-really-means/152212.
82 *Nazario, Jose, Estonian DDoS Attacks – A summary to date, Arbor Networks, available at: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.*
83 Cabinet Approves Action Plan to Fight Cyber-attacks. http://www.ria.ee/index.php?id=28731.
84 Estonia has so far convicted only one 20-year-old hacker. Dmitri Galushkevich used his home computer to bring down Reform Party's website. Read more e.g. Sachoff, Mike, Man Convicted In Estonia Cyber Attack, WebProNews, 24.01.2008. http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack (25.05.2008).
85 Mõttus, Kristiina, Naši komissar: küberrünnak Eesti vastu näis ainuõige sammuna. http://www.postimees.ee/290507/esileht/siseuudised/263405.php.
86 See e.g. Rand, Erki, Laar: suutlikkus Venemaa küberrünnakud tõrjuda on tõstnud Eesti mainet, Eesti Päevaleht, 11.07.2007. http://www.epl.ee/artikkel/392744.
87 Evron, Gadi; Aarelaid, Hillar. Estonia: Information Warfare and Lessons Learned. [2007] Available at: http://ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/s5_gadi_evron.pdf .
88 Kremlin-backed group behind Estonia cyber blitz. http://balticbusinessnews.com/Print.aspx?PublicationId=b737410e-e519-4a36-885f-85b183cc3478.

(CERT-EE) became the coordinating body for response to the attacks, engaging local service providers and a network of IT professionals on a voluntary basis from both the governmental and commercial sector, and experts both within and outside of the country.[89] The CERT's emergency response program involved analysing the severity of the incident, sending abuse reports to service providers abroad, and facilitating information exchange between the affected organisations and service providers.[90] Some assistance, primarily in the form of consultation, was also received from international organisations such as NATO.

It was however noted that even though the Estonian CERT was able, to a degree, to mitigate the impact of the attacks, due to the *ad hoc*, unofficial status of its tasking, it lacked the authority to enforce its recommendations on all parties involved.[91]

Regardless of the malicious attacks against Estonian web pages, Estonia tried to keep up domestic Internet traffic and visits to foreign web pages were mostly possible. Whilst most public sector web pages were accessible to domestic users, restrictions applied to Internet users abroad.[92]

THE LEGAL, POLICY AND ORGANISATIONAL RESPONSE: POST-2007 DEVELOPMENTS IN THE FIELD OF CYBER SECURITY

The 2007 attacks triggered modifications in the Estonian legislative situation and institutional landscape or in some cases supported or enhanced the changes already under way. Some of these changes were materialised over the period of 2007-2010, some still continue to be implemented.

The cornerstone of the recent developments is the national Cyber Security Strategy, adopted in May 2008.[93] In order to achieve the goals set in the strategy, a set of implementation documents has been approved that foresee a number of concrete measurable actions within the high priority areas of critical information infrastructure protection, overall competence of information security, relevant legal framework, international cooperation and awareness of cyber security issues.

89 Tiks, Oliver. 'Küberrünnakuid tõrjuvad sajad spetsialistid' (In Estonian). Postimees Online, 2 May 2007. Available at http://www.tarbija24.ee/120507/esileht/siseuudised/258274.php.
90 Evron, Gadi. 'Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War'. *Georgetown Journal of International Affairs,* Winter/Spring 2008, p 123.
91 *Ibid.*
92 'Malicious cyber attacks against Estonia come from abroad'. Press release by the Estonian Informatics Centre, http://www.ria.ee/index.php?id=28623.
93 For a more detailed introduction into the Estonian Cyber Security Strategy, see section 5.3.1 of this paper.

The strategy identified three legal fields in need of immediate review and updating: the legal regulation for tackling cyber crime, supporting the availability of CIIP, and indicating information security standards for critical information systems. Deriving from there, the main legislative changes encompassed two major legal acts: the Penal Code, where both substantive and procedural law amendments were adopted by the Parliament in March 2008, and the new Emergency Act (adopted in 2009), which now accommodates threats to critical information infrastructure.

In 2010, the Estonian Informatics Centre (EIC), a central government body responsible for government information systems as well as the Estonian national CERT, was supplemented by a new entity: Department for Critical Information Infrastructure Protection (CIIP)[94]. The tasks of the new department include creating a defence system for Estonia's critical information infrastructure and the protection of important IT systems of the public and private sectors alike. In May 2010, the government announced its intention to upgrade the Estonian Informatics Centre into a national cyber security organisation with full a mandate to exercise regulatory powers.[95]

The main developments in the fields of law, policy and organisational structure that were undergone after the 2007 attacks are discussed in more detail below.

CYBER SECURITY RELATED AMENDMENTS IN THE ESTONIAN LEGAL FRAMEWORK

Penal Code

In the aftermath of the 2007 cyber attacks, the terminology, elements and definitions of cyber crime in the Penal Code were thoroughly revised by several amendments. The reasons for the revision originated mostly in the need to harmonise the Estonian Penal Code with the Council of Europe Convention on Cybercrime[96] and the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[97], and to update the definition of "Acts of terrorism" (§ 237 of the Penal Code) in order to ensure its comprehensiveness and applicability to the cyber domain.

94 Kriitilise informatsiooni infrastruktuuri kaitse osakond (KIIK).
95 Infosüsteemide arenduskeskus saab võimu juurde, Postimees online, available at: http://www.postimees.ee/?id=262349.
96 http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
97 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systemshttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT.

Taking into account the complications that arose in the prosecution of the 2007 spring cyber attacks, the Ministry of Justice prepared a comprehensive amendment package to the Penal Code which was presented to the *Riigikogu* (Estonian Parliament) in December 2007 and adopted as law in February 2008.[98]

The amendments itemised in more detail the provisions of the Penal Code relating to attacks against computer systems and data, updated the extent of some provisions (such as adding the dissemination of spyware and malware) and added a new provision on preparation of cyber crimes. Based on the understanding that the frequency of cyber attacks has been on a steady rise, and that due to the rising availability of Internet and growing use of electronic channels by the population such attacks are becoming increasingly dangerous, the amendments also prescribed higher maximum punishments and corporate liability for such crimes.

Crimes against Computer Data and Computer Systems

The amendments[99] approved in 2008 followed the wording and structure of the Convention on Cybercrime by clearly distinguishing the two clauses § 206 "Interference in computer data" and § 207 "Hindering the operation of computer system" which previously had been combined in one paragraph. The text of the provisions as amended now stands:

§ 206 "Interference in computer data"

Illegal alteration, deletion, damaging or blocking of data or programmes within computer systems, or illegal uploading of data or programmes into computer systems is punishable by a pecuniary punishment or up to three years of imprisonment.

§ 207 "Hindering the operation of computer system"

Illegal interference with or hindering of the operation of a computer system by way of uploading, transmitting, deleting, damaging, altering or blocking of data is punishable by a pecuniary punishment or up to three years of imprisonment.

Whereas § 206 does not require any damage to be caused to qualify as "Interference in computer data", acts criminalised under § 207 need to involve an actual hindrance of and subsequent damage to a computer system. Similarly

98 The last available English translation of the Estonian Penal Code dates back to April 2008 and is available at the website of the Estonian Ministry of Justice at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik.

99 Karistusseadustiku muutmise seaduse eelnõu 166 SE II-1. http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20100318225035&file_id=256023&file_name=166s-XI.doc&file_sise=32256&mnsent=166+SE&fd=01.12.2009 (in Estonian).

to the Convention, § 207 outlines the possible ways of hindering the operation of a computer system, including damaging, deletion, deterioration, alteration or suppression of computer data without right. Thus, the new wording clarifies the possible elements of the crime and covers such acts as DoS, DDoS, and spamming. The paragraph also prevents qualifying any type of interference such as physical damaging or destruction of the computer systems or cables under § 207.

Additionally, the amendments resulted in increasing the level of punishment for certain acts under § 206, § 207, § 217, namely for attacks aimed against the computer systems of critical infrastructure. Critical infrastructure is defined and the objects of critical infrastructures listed in the Emergency Act (see section 5.2.3 of this paper).

Article 6 of the Cyber Crime Convention that regulates the misuse of computer devices was, prior to 2007, essentially uncovered by the Estonian Penal Code. After the adoption of the 2008 amendments, the new § 216[1] "Preparation of computer-related crime" asserts criminal responsibility for preparatory acts that are intended to be used for the purpose of committing any of the offences established in § 206, 207, 208, 213 or 217 of the Penal Code. These include the production, owning, distribution or otherwise making available of equipment, programs, codes or other data for accessing a computer system and using, distribution or otherwise making available of data necessary for committing the abovementioned crimes.

Computer Virus, Malware and Spyware

The aim of Article 4 in the Convention on Cybercrime is to provide computer data, computer programs and systems with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The input of malicious code, such as viruses, Trojan horses, malware and spyware is, therefore, covered under the Convention Article 4 "Data interference" as the acts result in the modification of data.[100]

§ 208 in the Estonian Penal Code originally exclusively addressed dissemination of computer viruses. The provision was later extended to include malware and spyware. The difference compared with § 206 "Interference in computer data" lies within the fact that using malicious code, viruses, malware, spyware and the kind does not imply the actor's active interference in the data of a computer system. The actor does not physically alter the data; rather, it is done by the malicious program.

It is interesting to note that § 208 regulates only the dissemination of computer

100 See the Explanatory Report to the Council of Europe Convention on Cybercrime. http://conventions.coe.int/treaty/en/reports/html/185.htm.

virus, malware and spyware, whereas § 216[1] criminalises the preparation of such programs.

Similarly to the previously mentioned clauses, the new wording of § 208 involves more severe sanctions for computer-related crime. Committing an act qualifiable as § 208 is punishable by pecuniary punishment or up to 3 years' imprisonment (compared to the 1-year imprisonment foreseen previously). If the same act is committed repeatedly, i.e. at least for the second time, or causes significant damage, the punishment can be a pecuniary punishment or up to 5 years' imprisonment.

Acts of Terrorism

Under the law prior to the 2007 attacks, Penal Code § 237 "Acts of terrorism"[101] read as follows:

> *Commission of a criminal offence against international security, against the person or against the environment, or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population is punishable by five to twenty years' imprisonment, or life imprisonment.*

In 2008, the § 237 of the Penal Code was amended to include "interference with computer data or hindrance of operation of computer systems as well as threatening with such acts'.[102] According to the new wording, an act of cyber crime, if motivated by terrorist aims and fulfilling the elements listed above, should be treated as terrorist crime by the Estonian law.[103]

The amended § 237 filled an important gap in the Penal Code by enabling differentiation between cyber attacks against critical infrastructure (with the purpose of seriously interfering with or destroying the economic or social structure

101 See also Explanatory note on the amendment of Penal Code. http://www.riigikogu.ee/?page=pub_ooc_file&op=emsplain&content_type=text/html&file_id=198499.
102 Estonian Penal Code (RT I 2001, 61, 364; 2009, 39, 261), § 237.
103 Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code (116 SE). (In Estonian.) December 2007. Available at: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20090902161440&file_id=198499&file_name=KarS%20seletuskiri%20(167).doc&file_size=66048&mnsensk=166+SE&etapp=03.12.2007&fd=29.10.2008.

of the state) and ordinary computer crime. A cyber attack against a country can disturb the functioning of the public authority or the provision of public services and it is therefore necessary to guarantee additional protection deriving from the criminal law. The provision also covers those possible cases of cyber terrorism where politically or socially motivated serious attacks against data or computer systems may result in severe economic loss or bloodshed.

Amendments Relevant to Procedural Law

The above-mentioned amendments in the Penal Code were partly brought about by the legal limitations that arose from the application of criminal procedure law[104] in co-effect with the Estonian Surveillance Act.[105]

As the investigation and identification of the originators of the attacks is always dependent on legally permissible measures, one of the founding applicable legal acts in the investigational matters is the Estonian Surveillance Act. According to the act, collecting information concerning data communicated via electronic communications networks is permitted only to surveillance agencies within the limits of their competence and within procedures authorised by law.[106] Thus, unauthorised surveillance, for example the unauthorised observing of a person's activities in order to collect information relating to that person, is criminalised and punishable by law.[107] According to the Act, monitoring and analysing data logs with the objective of identifying particular attackers does not belong to the competence of ISPs or CERT-EE and is reserved to law enforcement agencies.

§§ 110-112 of the Code of Criminal Procedure state that evidence may be collected by surveillance activities in a criminal proceeding if the collection of evidence by other procedural acts is a) precluded or especially complicated and b) the criminal offence under investigation is, at the minimum, an intentionally committed crime for which the law prescribes a punishment of at least three years' imprisonment.[108] Still, almost none of the criminal acts committed during the Estonian cyber attacks managed to meet the 'three years' imprisonment as punishment'-level.

104 Code of Criminal Procedure (RT I 2003, 27, 166; 2010, 40, 239). An unofficial English translation is available at http://www.legaltext.ee/text/en/X60027K6.htm.
105 RT I 1994, 16, 290; 2009, 62, 405. An unofficial English translation is available at http://www.legaltext.ee/text/en/X30011K7.htm
106 These are the Security Police Board, Police and Border Guard Board, the Military Police, the Prisons Department of the Ministry of Justice and prisons, and the Tax and Customs Board. *See* § 12 (1) section 5, § 6 (1) and (2) of the Estonian Surveillance Act.
107 § 137 of the Estonian Penal Code. Penal Code of Estonia (RT I 2001, 61, 364; 2009, 39, 261). An unofficial English text is available at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik.
108 § 110, 117 of the Estonian Code of Criminal Procedure.

The punishment prescribed by the 2007 Penal Code was pecuniary punishment or a maximum one year of imprisonment[109] and that disabled the applicability of surveillance activities.

Since collecting of evidence is complicated in investigating such crimes, the Penal Code amendments concerning the extension of the term of punishment for computer-related crimes to up to three years, made the use of surveillance measures available for the police.[110]

New Emergency Act

A part of the response to improve national resilience to cyber threats was the new Emergency Act[111] adopted in June 2009. For the purpose of drafting the new Act, an inter-ministerial working group was set up under the lead of the Ministry of the Interior in the spring of 2008, tasked with identifying critical infrastructure – including critical information infrastructure – and reviewing and updating the current setup of emergency preparedness in Estonia. Cyber security experts from different government agencies were involved in the project from the beginning.

The purpose of this undertaking, however, was wider than merely addressing cyber threats. Rather than following a segmented approach, the act was to comprehensively address all national emergency situations, laying a foundation for a uniform organisational emergency handling structure and procedural framework for emergency response. National *cyber security* threats were thus included under the general framework set up by the act; certain provisions also specifically address threats against information systems.

The act regards as 'emergency' those events which endanger, on a significant scale, the life or health of people, or cause significant proprietary or environmental damage, or cause severe and extensive disruptions in the continuous operation of vital services, and require prompt coordinated activities of several agencies in response. The definition is effect-based (the criteria being death and injury of people or destruction of property) rather than source-based – it does not differentiate whether the effect was caused by human, technological or natural

109 Penal Code, § § 206-208. For some cases involving severe damages or a previous offence of the same kind, an elevated term of punishment applied.

110 Explanatory Memorandum to the Draft Act on the Amendment of the Penal Code (116 SE). *(In Estonian.)* December 2007. Available at: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20090902161440&file_id=198499&file_name=KarS%20seletuskiri%20(167).doc&file_sise=66048&mnsensk=166+SE&etapp=03.12.2007&fd=29.10.2008.

111 RT I 2009, 39, 262; 2010, 24, 115. An unofficial English translation by the Ministry of Interior is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26&keel=en&pg=1&ptyyp=RT&tyyp=X&query=h%E4daolukorra.

factors – and encompasses also events where such consequences are brought about by cyber activities. The definition does not *per se* differentiate whether the emergency is caused by hostile actors (threats) or results from structural conditions or accidents without relation to intent or capabilities of actors (risks).

For the purpose of response, the act foresees a system of measures which includes *preventing* emergencies, *preparing* for emergencies, *responding* to emergencies and *mitigating* the consequences of emergencies ('crisis management').

The responsibilities of emergency response are divided between relevant stakeholders – while the national crisis management committee[112] is responsible for national scale coordination and ensuring emergency preparedness, a system of regional and local committees[113] was set up for operational crisis management in emergency situations of regional or local scale, with the task to ensure the continuity of certain vital services and act as coordinating bodies.

The protection of critical infrastructure – including critical information infrastructure – is addressed in Chapter 4 of the Emergency Act. The chapter identifies 41 services essential to public security, public safety, and the economic and social welfare of people. It also specifies the requirements for ensuring the continuous operation of these vital services and the division of tasks between stakeholders for this purpose.

Management and coordination functions for ensuring sectoral service continuity are divided between different ministries in accordance with their spheres of competence, with the Ministry of the Interior functioning as the central coordinating body. Their purpose is to ensure the following:

a) avoiding wide-scale disruption of the continuous operation of vital services *(prevention)*;

b) the availability of sufficient measures to swiftly eliminate disruptions or launch alternatives *(reaction)*;

c) adequate preparedness of both public and private sector to restore the continuous operation of vital services *(consequence management)*.[114]

The task of individual ministries is to coordinate emergency preparedness activities, advise and supervise the actual entities providing vital services, and keep the Ministry of Interior regularly updated about the situation in their area of

112 The crisis management Committee of the Government of the Republic. The Committee is a permanent body under the Government, chaired by the Minister of the Interior; its members are appointed by the Estonian government. The tasks of the Committee are defined in § 3 of the Emergency Act.

113 § § 4 and 5 of the Emergency Act, respectively.

114 Ministry of the Interior, Department of crisis management and rescue policy. Elutähtsad valdkonnad ja teenused. http://www.siseministeerium.ee/elutahtsad-valdkonnad-ja-teenused-2/ (In Estonian).

responsibility.

The "top layer", i.e. ministry-level management tasks related to ensuring services that are vital for the functioning of information society is divided among different ministries according to their daily competence share; there is no body specifically appointed with the managing the continuity of information infrastructure-related services across service sectors. Overseeing the continuous functioning of communications networks – including fixed and mobile telephone networks, data communications networks, and cable television networks – lies within the sphere of competence of the Ministry of Economic Affairs and Communications.

However, the act also places a burden of day-to-day emergency prevention and ensuring service continuity on providers of public services such as energy suppliers, hospitals, and, relevant to cyber security, electronic communications service providers and information infrastructure owners.

Providers of vital services, i.e. agencies or legal persons that fulfil a public administration duty defined as a vital service in Chapter 4 or undertakings that provide a vital service listed in Chapter 4 have four main legal obligations regarding emergency preparedness:

1) obligation of preparing and presenting a continuous operation risk assessment[115];
2) obligation of preparing and presenting a continuous operation plan[116];
3) obligation of notification regarding events significantly disturbing service continuity or an impending risk of the occurrence of such events;
4) obligation to provide information to supervisory bodies upon the latter's request.

The continuous operation risk assessments and continuous operation plans are to be presented, for the first time, by 1 January 2011. Uniform guidelines for preparing both of these documents were established by the Minister of the Interior in June 2010.

A separate provision stipulates the obligation of each provider of a vital service to ensure the continuous application of security measures with regard to the

115 See § 38 of the Emergency Act. A *continuous operation risk assessment* is a document describing the *risks* causing a partial or complete interruption in the provision of vital services, the *probability* for such an event, and the *possible consequences* of a partial or complete interruption in the provision of the vital service. The risk assessment is to be regularly assessed for up-to-dateness and amended as necessary.

116 See § 39 of the Emergency Act. A *continuous operation plan* is a document describing the *measures* that need to be taken to prevent and mitigate partial or complete interruptions in the provision of vital services and restore the continuous operation of vital services in the event of a disruption.

information systems used for the provision of vital services, and related *information assets*. The requirements for such specific security measures for vital service information systems and related information assets are to be established by the Government of the Republic by January 2011.

Legislative Review: a Summary

A legal framework that fully supports the objectives of a secure information society needs to comprehensively cover several aspects of law belonging to different legal disciplines. These can be illustrated by the following graph:

CONSTITUTIONAL LAW

FUNDAMENTAL RIGHTS AND FREEDOMS;
ORGANISATION OF THE STATE;
EXECUTION OF PUBLIC AUTHORITY

PRIVATE LAW	PUBLIC ADMINISTRATIVE LAW	CRIMINAL LAW	CRISIS MANAGEMENT LAW	WAR-TIME LAW / NATIONAL DEFENCE LAW
Information society services	General administrative procedure law supporting the accessibility of information society	Substantive criminal law	Critical infrastructure protection (CIP)	National defence organisation
eComms infrastructure provision	Availability of public information and public e services	Criminal procedure law	Critical information infrastructure protection (CIIP)	National defence in peacetime
Provision of eComms services to end users	Data processing and data protection	International cooperation		National defence in conflict/ wartime
General private law supporting the functioning of information society (eCommerce, digital signatures)				

As appears from the division above, the post-2007 legal amendments involved most

of the fields of law depicted, most substantially criminal law (including aspects of criminal procedure) and crisis management law. While not directly involving the second column of the graph above, these amendments are closely tied to it, aiming to strengthen the accessibility of information society as well as the availability of public information and public e-services.

In parallel to the review of crisis management law, the Ministry of Justice was tasked[117] to revise the State of Emergency Act[118] which addresses the preparation for and response to emergencies arising from military threat. This task was chiefly undertaken to ensure the up-to-dateness of the State of Emergency Act in the changed legal and factual environment since the adoption of the act in 1996 – concerning which the street riots and cyber attacks of spring 2007 served as a major wake-up call – but also to ensure consistency between the laws dealing with non-military (Emergency Act) and military threats (State of Emergency Act).

Some updates were also required in legal acts usually classified as private law – in this case, the Electronic Communications Act. The amendment concerned the keeping of log files for online user activities (the so-called data retention obligation foreseen by the European Union data retention directive[119]). Namely, the relevant provisions in the Electronic Communications Act which were intended to ensure that data is retained with regard to the source, destination, date, time and duration of a communication concerning, among other, Internet access, Internet e-mail and Internet telephony, foresaw no liability for cases where communications undertakings failed to meet this obligation. Neither was this liability included in other acts, such as the Penal Code. In practice, this often meant that log files that were required by the police for pre-trial criminal proceedings were either missing or the data contained therein was unreadable.[120] With the amendment, the relevant liability was added in § 184[1].

117 Explanatory Memorandum to the draft act, section 2: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/rtf&file_id=574992&file_name=ErSS%20ja%20KMS%20muutmine%20seletuskiri%20(449).rtf&file_sise=36279&mnsensk=448+SE&fd=2010-04-22 (in Estonian).

118 Erakorralise seisukorra seadus (RT I 1996, 8, 165; 2009, 39, 260). Unofficial English text of the act is available at: http://www.legaltext.ee/text/en/XX10024.htm (update pending).

119 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. OJ L 105, 13.4.2006, pp. 54-63.

120 Explanatory Memorandum to the Act amending the Electronic Communications Act (424 SE) (In Estonian), available at: http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=535868&file_name=elektroonilise%20side%20muutmine%20seletuskiri%20(424).doc&file_sise=31650&mnsensk=424+SE&fd=2010-04-22.

POLICY

The policy response to the cyber attacks has been diverse: Estonia has initiated several national projects with great significance[121], fostered international cooperation with a number of international organisations[122], as well as paid more attention to the regulation of information society as a whole.[123]

Partly in response to the attacks, and partly due to already undertaken initiatives, the government was determined to outline the Estonian Information Society Strategy 2013[124] and the Implementation Plan 2007-2008 of the Estonian Information Society Strategy[125], as well as draft the Estonian Cyber Security Strategy[126] with a set of additional implementation documents. Additionally, since 2007, elements of the cyber security domain and the need for a more effective regulation have been increasingly mentioned in the strategies of other domains, such as the Guidelines for Development of Criminal Policy until 2018[127] and its explanatory documentation[128] that define long-term objectives and activities on the basis of which the public sector shall plan and perform its activities.

Adopting the Cyber Security Strategy

The adoption of the Cyber Security Strategy has been probably one of the most important undertakings in terms of national security since 2007. The committee in charge of the drafting and adoption of the document consisted of a number of public institutions such as the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Economic Affairs and Communications,

121 List of IT-related projects in Estonia, RISO, available at: http://www.riso.ee/en/information-policy/projects.
122 E.g. Estonia Supports Council of Europe in Fight Against Cyber Crime, Estonian Ministry of Foreign Affairs press release, available at: http://www.vm.ee/?q=en/node/9315; Foreign Minister Paet Invited EU and Southeast Asian Nations to Co-operate in Backing Cyber Defence, Estonian Ministry of Foreign Affairs press release, available at: http://www.vm.ee/?q=en/node/9512; National Experts Shared Cyber Security Recommendations with UN Secretary General, Estonian Ministry of Foreign Affairs press release, available at: http://www.vm.ee/?q=en/node/9722.
123 E.g., Cyber Security Strategy, Information Society Strategy 2007-2013. See more, 5.3.1, 5.3.2.
124 Estonian Information Society Strategy 2013, available at: http://www.epractice.eu/files/media/media_186.pdf.
125 Implementation Plan 2007-2008 of the Estonian Information Society Strategy. Available at http://www.riso.ee/en/information-policy/policy-document/implementation_plan.
126 'Cyber Security Strategy'. Cyber Security Strategy Committee, Ministry of Defence. Tallinn 2008. The English version of the Estonian Cyber Security Strategy is available at: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.
127 Guidelines for Development of Criminal Policy until 2018, available at: http://www.just.ee/orb.aw/class=file/action=preview/id=50603/Kriminaalpoliitika+arengusuunad+aastani+2018.pdf.
128 Explanatory documentation to Guidelines for Development of Criminal Policy until 2018, available at: http://www.just.ee/orb.aw/class=file/action=preview/id=50604/Seletuskiri+(kriminaalpoliitika+arengusuunad+aastani+2018).pdf.

the Ministry of Internal Affairs and the Ministry of Education and Research. [129] The implementation and overall efficiency of the strategy will be assessed by the Cyber Security Council of the Security Committee of the Government of the Republic.[130] The strategy was presented to the Government and adopted in May 2008.

The practical implementation of the strategy is described in more detail in the implementation plans, which focus on the concrete actions and funds needed to achieve the goals of the Strategy in four main areas: protection of critical information infrastructure and establishment of relevant national systems; increasing competence in cyber security; formation of legal framework for ensuring cyber security; bolstering international co-operation, and raising awareness on cyber security. An Implementation Plan of the strategy for the period of 2008–2010 was compiled, taking into account the suggestions from different state agencies, interest groups and committees, and adopted in May 2009.[131]

In a nutshell, the strategy underlines that the asymmetric security risk of cyber attacks results in inherent vulnerabilities of cyberspace and reflects a global issue that can effectively be solvable only by coordinated actions of all nations. The strategy suggests implementing organisational, technical and regulatory information security measures, as well as aims to developing an over-arching and sophisticated *cyber security culture*.[132]

The strategy aims to fulfil five strategic policy objectives[133]:

a) The development and large-scale implementation of a system of security measures;

b) Increasing competence in cyber security;

c) Improvement of the legal framework for supporting cyber security;

d) Bolstering international cooperation; and

e) Raising awareness on cyber security.

Information Society Strategy 2007-2013

In July 2009, the Government of Estonia approved the amended version of the

129 'Cyber Security Strategy'. Cyber Security Strategy Committee, Ministry of Defence. Tallinn 2008. The English version of the Estonian Cyber Security Strategy is available at: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.
130 *Id.*
131 'Valitsus kiitis heaks küberjulgeoleku strateegia rakendusplaani aastateks 2009–2011'. Postimees, 14 May 2009 *(In Estonian).* Available at: http://uudisvoog.postimees.ee/?DATE=20090514&ID=204872.
132 'Cyber Security Strategy', p. 3.
133 *Id.*, p. 27-34.

"Estonian Information Society Strategy 2007-2013"[134], an updated policy paper, the first version of which had already been adopted by the government in 2006. The update mainly concerned the measure identified in its section 4.1.1, "Broadening technological access to digital information", to which a chapter was added on the development of broadband Internet access (the EstWIN project[135]).

In 2010, the Implementation Plan for 2010-2011 of the Estonian Information Society Strategy 2007-2013 followed. The document sets out six priority areas: increasing the knowledge, skills and participation of individuals; development of Estonia's next generation broadband network; development of electronic business environment; development of public services; large-scale uptake of e-ID; increasing the interoperability of state information systems. Implementation plan for the years for 2011–2013 is currently under development.

National Security Concept of Estonia

The National Security Concept of Estonia[136] was approved by the Parliament in May 2010, replacing the previous version from 2004. The framework document introduces the objective, principles and directions of the security policy, and emphasises among other global security developments the growing dependence of countries' resilience on the use of cyberspace.[137] As cyberspace may well be used to incite tension and conflicts within a nation, the importance of sufficiently protecting the information technology and communications systems is underlined. The concept separately mentions the need for preventing and combating cyber crime by the means of enhanced cooperation between agencies, developments on legislation and endorsement of public awareness.[138]

134 *Supra note* 64.
135 The objective of the Estonian Broadband Development Foundation (founded in 2009 by the initiative of Ministry of Economic Affairs and Communications and by the members of Estonian Association of Information Technology and Telecommunications) is to launch the project EstWin and give all residential houses, businesses and authorities the possibility to connect to the next-generation broadband network with a transmission speed up to 100 Mbit/s by the year of 2015. "In the scope of EstWin project more than 6000km of fiber-optical cables will be installed and more than 1400 connection points will be constructed. The construction of basic network should provide that 98% of the residential houses, businesses and authorities are located closer than 1.5 km from the basic network". Read more, Estonian Broadband Development Foundation, available at: http://www.elasa.ee/.
136 National Security Concept of Estonia (2010), available at: http://www.kmin.ee/files/kmin/nodes/9470_National_Security_Concept_of_Estonia.pdf.
137 *Id.* p. 6.
138 *Id.* p. 17.

REVIEWING THE ORGANISATIONAL FRAMEWORK

Estonian Informatics Centre

Organisation of the Estonian Informatics Centre

The Estonian Informatics Centre is a state agency administered by the Ministry of Economic Affairs and Communications (MEAC) in general coordination of state information policy and public sector IT development as defined in the national strategy for information society development[139].[140]

The core tasks of the Centre are the coordination of execution of development plans for Estonian information society, development and administration of the components supporting state information systems and ensuring their security, and coordinating incident handling Estonian in computer networks. Since September 2009, the Centre is also responsible for managing and coordinating activities related to the information security of state information systems and Estonian critical information infrastructure. The Centre is the core body responsible for the functioning of information society services provided by the state and the development and administration of intra-governmental data communications services and infrastructure. Additionally, the Centre is the national implementing body for European Union structural aid programs.

The Centre consists of six departments, one of which is the Estonian Computer Emergency Response Team (CERT-EE), and another deals with critical information infrastructure protection.

CERT-EE and Its Role

The Computer Emergency Response Team of Estonia (CERT-EE) has, since its setup in 2006, been the entity responsible for the management of security incidents in .ee computer networks and the national contact point for international co-operation in the field of IT security. CERT operationally handles security incidents that take place in Estonian computer networks, takes measures to prevent such incidents, and works to raise the security awareness of end-users. On state level, CERT's tasks are performed by the Department for Handling Information Security Incidents of the Estonian Informatics Centre.[141]

139 Estonian Information Society Strategy 2013, *supra note* 64.
140 See also the introduction provided at the website of the Estonian Informatics Centre: http://www.ria.ee/about.
141 CERT Estonia, available at: http://www.cert.ee/.

In the 2007 cyber attacks, the CERT naturally became the coordinating body for response to the attacks, engaging system administrators and experts both within and outside of the country. While the legal categorisation of the incident and the suitable legal remedies were still discussed, technical measures such as increasing the bandwidth of affected targets and filtering out malicious traffic were applied as measures available under the Electronic Communications Act in cases of harmful interference and negative effects to the integrity of communications networks.[142] These activities were carried out by network and service providers in close cooperation with the CERT.

Even though the technical coordination in incident handling worked well *ad hoc*, questions nevertheless remained unanswered. The authority to coordinate response to or recovery from major cyber attacks was divided between different government entities. The CERT is subordinated to the MEAC. The coordination of matters related to terrorism has so far been the concern of the Ministry of Internal Affairs, while national security matters are handled mainly by the Ministry of Defence. In order to avoid conflicting responsibilities and ensure a streamlined response, the coordination needs to be based on a clear legal regime. As the foundation for a coherent response framework was established with the new Emergency Act in 2009 (see the discussion under section 5.2.3 of this paper), the implementation of the Act will continue to place a stronger burden on the CERT and the Estonian Informatics Centre in general, especially on its department of critical information infrastructure protection.

Department of Critical Information Infrastructure Protection

Due to the adoption of the Emergency Act and the necessity for a competent body to advise and coordinate the matters of protection of critical information infrastructure, the Estonian Informatics Centre was expanded by a new entity – the department of Critical Information Infrastructure Protection (CIIP Department). While the advisory function had *de facto* been fulfilled by the Centre already prior to the setup of the new unit, the Centre now had dedicated staff[143] and a clear-cut tasking to manage and coordinate the creation and operation of a defence system for Estonia's critical information infrastructure.

The CIIP Department is to deal with the protection of important IT systems of the

142 § § 98 and 127 of the Electronic Communications Act. Unofficial English translation available at: http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=X90001K2.htm&query=elektroonilise%20side&tyyp=X&ptyyp=RT&pg=1&fr=no.

143 As of the start of the department in October 2009, the staff included two people (head of department and a risk manager), with plans to increase the number of staff in future.

public and private sectors alike, coordinating general prevention and response activities while the owners of each vital service concerned remain responsible for the daily defence of their systems. According to Toomas Viira, head of the department, the setup of the new department was called by a need for a central unit to analyse the threats and risks against various information services vital to the state, as well as the influence of various IT systems on one another. The CIIP Department will be able to give recommendations on improving the defence of information systems.[144]

Compared to the more operational role of CERT-EE, the CIIP Department will function at a more strategic level, and thus complement the existing capabilities of the Estonian Informatics Centre to include a fuller competence.

Restructuring the Estonian Informatics Centre

In May 2010, the Government supported the proposal of the Ministry of Defence to reform the Estonian Informatics Centre, upgrading it from a ministry-administered state agency into a government agency with autonomous executive powers.[145] The new regulatory body is to be better empowered to enforce the principles defined by the national cyber security strategy, thus ensuring a greater degree of coherence and better efficiency in its implementation.

According to the Minister of Defence quoted in the article cited above, the tasks of the new authority would comprise monitoring and regulating undertakings that own and run critical information infrastructure, as well as supervising other governmental agencies dealing with information infrastructure. Granting additional mandate to the Estonian Informatics Centre would serve as a long-term investment for cyber security in Estonia, both in terms of ensuring a higher level of information security on the national scale and facilitating international cooperation in the field.

The name of the new governmental organisation and the number of new staff to be recruited is not yet fully determined, but there is an initial agreement that the reform would be completed and the new body launched by January 2011.

Cyber Defence League

The cyber events in April-May 2007 awakened a discussion in Estonia about the potential role for voluntary efforts of defending information infrastructure in the

144 EIC creates unit for defence of critical information systems. Press release by the Estonian Informatics Centre, 30 Sept 2009. http://www.ria.ee/eic-creates-unit-for-defence-of-critical-information-systems.
145 Pesur, Veiko, Infosüsteemide arenduskeskus saab võimu juurde, Postimees Online, 13 May 2010, available at: http://www.postimees.ee/?id=262349.

event of cyber attacks. The concept received support in the 2008 Cyber Security Strategy, and first units of the Cyber Defence League (also *CDL*) were activated in early 2009.[146]

The Cyber Defence League operates as a part of the Defence League, a voluntary military national defence organisation founded already in 1918 (and restored in 1990) whose traditional purpose has been to enhance the readiness of the nation to defend its independence and its constitutional order, including in the event of military threat, but also by supporting civil structures such as the rescue service and police.[147] The Cyber Defence League functions within the same framework, with a mission to protect the high-tech lifestyle of the country, defending information infrastructure and working to raise awareness, share best practices, improve cooperation (incl. across the private and public sector) and create a network of specialists that are able to support mitigation efforts in the case of a cyber incident.[148]

In addition to its routine daily task of improving awareness and competence, the Cyber Defence League can be used in emergency response, rescue work and in ensuring security. The conditions and procedure for their involvement are specified in the Emergency Act: the CDL may be used for performing emergency situation tasks, as well as preventing or restraining acts of terrorism (including via cyber means) and preventing or restraining the damaging of high-risk objects. The precondition for the CDL's involvement is the inability of a competent agency to perform the duty in a timely manner and the absence of other means to perform the duty; in any case, the CDL has to follow the procedure established by the Government of the Republic.[149]

The Cyber Defence League unites IT specialists in key positions, patriotically minded people with IT skills that are willing to make a contribution to the cyber defence of the nation, and experts of various other disciplines that support cyber defence.[150]

As of spring 2010, the Cyber Defence League included about 60 members.[151]

146 Jaagant, Urmas. Küberkaitseliit pakub harjutuskeskkonda vabatahtlikele IT-spetsialistidele. EPL Online, 14 April 2010. http://www.epl.ee/artikkel/575013.
147 See the introduction about the Defence League at http://www.kaitseliit.ee/index.php?op=body&cat_id=288.
148 *Küberkaitseliit*. National Defence League's website, http://www.kaitseliit.ee/index.php?op=body&cat_id=395; KKK. National Defence League's website, http://www.kaitseliit.ee/index.php?op=body&cat_id=396.
149 See § 31 of the Emergency Act (an unofficial English translation is available at http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=XXXXX26.htm&query=h%E4daolukorra&tyyp=X&ptyyp=RT&pg=1&fr=no).
150 See supra note 115.
151 Randlaid, Sven, Küberkaitseliit soovib oma liikmeskonda laiendada, ERR, 15 April 2010. http://uudised.err.ee/index.php?06200567.

CONCLUSION

High level of IT development and the inevitable dependency on information technologies determine the need to protect nations against cyber attacks, be they criminal or military by nature. Although the attacks in Estonia in 2007 were not *per se* regarded as cyber war, they made the Estonian authorities review the existing cyber security concept and come up with a comprehensive strategy for protecting the information society.

The attacks triggered modifications in the Estonian legislative situation, organisational structure as well as institutional landscape. Following the legal analyses undergone for the new cyber security strategy and the implementation plan, there were several changes made in the Penal Code. The modifications itemised in more detail the provisions relating to attacks against computer systems and data, updated the scope of some provisions (such as adding the dissemination of spyware and malware) and added a new provision on preparation of cyber crimes. The amendments also prescribed higher maximum punishments and corporate liability for such crimes.

The new Emergency Act was adopted to offer legal remedies and contingency planning for critical information infrastructure. The aim of the act is to comprehensively address all national emergency situations, laying a foundation for a uniform organisational emergency handling structure and procedural framework for emergency response. National cyber security threats were thus included under the general framework set up by the act. Certain provisions also specifically address threats against information systems.

From organisational perspective, the central governmental body responsible for government information systems as well as the Estonian national CERT, was supplemented by the Department for Critical Information Infrastructure Protection (CIIP). The tasks of the new department include creating a defence system for Estonia's critical information infrastructure and the protection of important IT systems of the public and private sectors alike. The Emergency Act will continue to place a stronger burden on the CERT and the Estonian Informatics Centre in managing cyber security.

The Cyber Defence League was created with a mission to protect the high-tech lifestyle of the country, defending information infrastructure and working to raise awareness, share best practices, improve cooperation (e.g. between the private and public sector) and create a network of specialists that are able to support mitigation efforts in the case of a cyber incident. It functions as a part of the Defence League, a voluntary military national defence organisation founded already in 1918 (and

restored in 1990) whose traditional purpose has been to enhance the readiness of the nation to defend its independence and its constitutional order, including in the event of military threat, but also by supporting civil structures such as the rescue service and police.

The analysis of the policy, legal and organisational aftermath of the Estonia 2007 cyber attacks concludes that in order to achieve a comprehensive set of effective measures for preparedness, response and mitigation in the field of cyber security and defence, the arguments deriving from all three fields of law – LOAC, Criminal Law and IT Law – must be combined in an over-arching response. Additionally, by engaging several areas of government in cyber security capability building and integrating policies and views on cyber security, Estonia has taken its cyber security planning and preparedness a level higher from the previous, information-society focused approach.

DIFFERENT LEGAL CONSTRUCTS FOR STATE RESPONSIBILITY

Maeve Dion [152]

Abstract

For most countries, effective national cyber security will require international cooperation in both the preparation for and mitigation of cyber incidents. Currently, interactions among international cyber incident responders are based on technical, operational, diplomatic, and political relationships, not legal relationships. Most existing international legal frameworks were established for incidents and crimes unrelated to the cyber context; they therefore may be inapplicable or inefficient to properly address and deter cyber incidents that threaten national or international security. National and international cyber security may be improved by establishing a legal framework for accountability, and by holding each country responsible for ensuring minimum levels of security and incident response capabilities and for taking reasonable efforts to mitigate cyber incidents conducted through its information infrastructures. However, before any new constructs or new laws are created, existing legal frameworks should be assessed to determine their appropriateness for managing global and international cyber threats.

BACKGROUND

With society's ever-increasing reliance on the global information infrastructure, cyber security has become a significant aspect of national and international security. Governments, economies, and societies rely on the telecommunications and computer systems that make up this internationally-connected information infrastructure. Such dependence creates vulnerabilities when the information infrastructure becomes a target or field of conflict. Wrongdoers may send a flood of electronic messages to a targeted computer system, causing the system to fail or slow to a crawl due to the heavy communications traffic. Attackers may target a utility company's industrial control systems,[153] causing damage not only to the

152 Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, Arlington, Virginia, U.S.A.

153 Electronic systems that control industrial processes (e.g., for water and wastewater, electric power, oil and natural gas, etc.).

utility company but also to its customers who lose service.

In the past several decades, governments have therefore broadened their traditional definitions of national security to incorporate protection of critical infrastructures, and particularly the computer systems of those critical infrastructures. For example, The Netherlands determined that "[c]ritical infrastructure refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage." In the United States, critical infrastructure includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." In Australia, "[c]ritical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."[154]

Because telecommunications and information systems are connected globally, however, critical infrastructure protection may not be achieved from merely a national approach; it also requires international strategy and coordination. For example, due to the structure of the Internet, a local cyber incident may originate from computers on another continent. The increasingly interconnected computer systems create the potential for a local event to cascade across geographical and sovereign borders. National security incidents in critical infrastructure computer systems may therefore have significant international components, requiring cooperation in efforts of prevention, mitigation, prosecution, and deterrence.

The need for an international effort has been voiced by various international organizations and governments. In 2009 the Council of Europe established an ad hoc advisory group to address legal constructs for state responsibility regarding protection of critical Internet resources and cross-border flow of Internet traffic.[155] The European Commission in 2009 issued a new communication on Protecting

154 These definitions, and others, are found in: Kathryn Gordon & Maeve Dion, *Protection of "Critical Infrastructure" and Role of Investment Policies Relating to National Security* (Organisation for Economic Co-Operation and Development, 2008) (background document to the OECD Secretariat in support of the OECD Roundtables on Freedom of Investment, National Security and 'Strategic' Industries, Paris, France), http://www.oecd.org/dataoecd/2/41/40700392.pdf, p. 4 (Table 1: National Definitions of Critical Infrastructure).

155 Ad hoc Advisory Group on Cross-border Internet. http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/default_en.asp.

Europe from Large Scale Cyber-Attacks and Disruptions, which emphasized the importance of international cooperation for cyber security, and included action items to help member states evolve from a purely national approach.[156] In mid-2008, the Organisation for Economic Co-Operation and Development (OECD) recommended that member countries conduct a systematic review of their laws and regulations relevant to critical information infrastructures, and asses the need for updates, new laws, or new enforcement / implementation regimes; develop a national cyber security strategy that incorporates all the requisite government jurisdictions and private sector operations; and coordinate with other member states and non-OECD countries to take into account interdependency vulnerabilities of the global information infrastructure.[157]

November 2009 saw the launch of Australia's first Cyber Security Strategy, which includes among its priorities: international engagement and effective legal and law enforcement frameworks. Along with the June 2009 update of its National Security Strategy, the United Kingdom released its first U.K. Cyber Security Strategy, for which one key priority was international coordination for the development of international law. The United States' 2009 Cyberspace Policy Review identified multi-jurisdictional legal analyses and international cooperation as two of the most urgent policy action-items.

In addition to international cooperation, cyber security requires a multidisciplinary focus that integrates technical, organizational, political, and legal solutions. Comprehensive legal and policy analyses must guide and support the organizational and technical solutions to security challenges. Although most government policymakers are not experts in technology or telecommunications, it is important that policies and laws are written with a firm understanding of the technology and business realities that sustain the critical infrastructures.

COMMON PERSPECTIVES

National and international recognition of cyber vulnerabilities have resulted in legal research on a variety of related topics. For example:

- Existing literature includes treatises on the cyber component of national

156 Available at http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf.
157 *See OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]*, at http://www.oecd.org/dataoecd/1/13/40825404.pdf.

security,[158] cyber crimes and torts,[159] and law enforcement techniques and forensics.[160] Experts have written texts on cyber crime activities within organized and transnational criminal networks,[161] as well as case studies of actual computer crimes.[162] There has been a degree of international agreement on cyber crime efforts,[163] with some calls for additional international activities such as the creation of new treaties.[164]

- Attention has been given to civil liberty protections,[165] societal issues,[166] and regulation and other business concerns.[167]
- The military community was one of the first to look at policy and legal impacts of the burgeoning information infrastructure, thus developing a relatively rich research portfolio on cyber warfare.[168] Currently there is a nascent effort to create an international manual on cyber warfare, along the lines of the San Remo Manual on International Law Applicable to Armed Conflicts at Sea and the more recent Commentary and Manual on International Law Applicable

158 *E.g.,* Susan W. Brenner, Cyberthreats: The Emerging Fault Lines of the Nation State (Oxford University Press 2009); Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (The National Academies Press 2003); Cybersecurity and Homeland Security (Nova Science Publishers 2006).

159 *E.g.,* Jonathan D. Hart, Internet Law: A Field Guide, Sixth Edition (BNA Books 2008); Michael Rustad, Internet Law in a Nutshell (West 2009); Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace (Praeger 2010).

160 *E.g.,* Bill Nelson, Amelia Phillips, & Christopher Steuart, Guide to Computer Forensics and Investigations, 4th Edition (Course Technology 2009); Anthony Reyes et al., Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors (Syngress 2007).

161 *E.g.,* Seymour E. Goodman & Abraham D. Sofaer, The Transnational Dimension of Cyber Crime and Terrorism (Hoover Press 2001).

162 *E.g.,* Byron Acohido & Jon Swartz, Zero Day Threat (Union Square Press 2008).

163 *E.g.,* the Council of Europe Convention on Cybercrime.

164 *E.g.,* AFP, "UN chief calls for treaty to prevent cyber war," The Australian (Feb. 1, 2010) (discussing comments by International Telcommunications Union secretary general Hamadoun Toure during a World Economic Forum) at http://www.theaustralian.com.au/australian-it/the-hub/un-chief-calls-for-treaty-to-prevent-cyber-war/story-fn4mm2dt-1225825397532.

165 *E.g.,* Human Rights and the Internet (Palgrave Macmillan 2000); Global Employee Privacy & Data Security Law (BNA Books 2009).

166 *E.g.,* Athina Karatzogianni, The Politics of Cyberconflict (Routledge 2006).

167 *E.g.,* W. Russell Neuman, Lee W. McKnight & Richard Jay Solomon, The Gordian Knot: Political Gridlock on the Information Highway (The MIT Press 1999).

168 *E.g.,* Richard W. Aldrich, "The International Implications of Information Warfare," Airpower Journal, pp. 99-110 (Fall 1996); U.S. Department of Defense Office of General Counsel, "An Assessment of International Legal Issues in Information Operations" (May 1999); Walter Gary Sharp, Sr., CyberSpace and the Use of Force (Aegis Research Corp. 1999); David J. DiCenso, "IW Cyberlaw: The Legal Issues of Information Warfare," Airpower Journal, pp. 85-101 (Summer 1999); Thomas C. Wingfield, The Law of Information Conflict (Aegis Research Corp. 2000); Greg Rattray, Strategic Warfare in Cyberspace (The MIT Press 2001); Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *Jus in Bello*," International Review of the Red Cross, Vol. 84, No. 846, pp.365-98 (June 2002); Cyberwar, Netwar and the Revolution in Military Affairs (Palgrave Macmillan 2006); Pia Palojarvi, A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict (Erik Castren Institute of International Law and Human Rights 2009).

to Air and Missile Warfare.

NOT WAR OR CRIME, BUT STILL A THREAT

Despite the relatively large bodies of work on cyber crime and warfare, only recently have legal researchers begun to recognize a legal "grey area" where an international cyber incident falls below the definitional thresholds of international humanitarian law and yet exceeds the traditional definitions, organizational structure, and deterrent effects of criminal law.[169] This is an area of national security concern, particularly regarding incidents in the computer systems of critical infrastructures. An example of such an incident would be "patriotic" efforts by individuals of Country A who are protesting actions by the government of Country B. These individuals may hack into the governmental or critical infrastructure computer systems of Country B. Alternatively, the protesting individuals may coordinate to flood Country B's government, financial, and media computer systems with so much electronic traffic that the systems fail or slow down so much as to be unusable.[170] Sabotage by protestors is not a new concept, but the situation is complicated by the digital ability to perpetrate sabotage from a distance, possibly anonymously,[171] and with the threat of cascading effects through the interconnected critical infrastructure computer systems.

If the cyber acts have been identified as crimes in a national penal code, the likely legal tools at Country B's disposal are traditional criminal law enforcement efforts and possibly a mutual legal assistance agreement with Country A. Of course, depending on the nature of their relationship, Country A may be reluctant to provide political or law enforcement assistance to Country B. An additional complicating factor is that due to the structure and nature of the Internet, the Country A protestors' malicious activity may be conducted via telecommunications systems beyond the immediate conflict (e.g., not just in Countries A and B, but also Countries X, Y, and Z). If Country B is prepared, it may have a Computer Emergency Readiness Team ('CERT'), and if it is lucky, Countries X, Y, and Z are friendly and have already established cooperative relationships between their CERTs and Country B. (It is important to note that Country B may be neither prepared nor lucky, since countries vary in their capabilities for cyber incident response, law enforcement, and intra- and inter-governmental coordination that may be required.)

169 *See* Eneken Tikk, Kadri Kaska & Liis Vihul, International Cyber Incidents: Legal Considerations (Cooperative Cyber Defence Centre of Excellence, 2010).
170 Called Distributed Denial of Services ('DDoS') attacks.
171 Due to the lack of high confidence in technically attributing an attack to a specific person, as well as a lack of high confidence (or international comfort) in identifying sponsorship of an attack to a specific nation.

The interactions among international cyber protectors and incident responders are mostly based on technical, diplomatic, and political relationships. There is no common, international law that requires other countries to help Country B, and thus there is no liability for failure to help. If the cyber incidents can be defined as armed conflict and can be attributed to specific country, then Country B may initiate actions under international humanitarian law. It should be noted that while traditional conflicts have included cyber components, to date no standalone cyber incidents (unattached to physical conflict) have been deemed armed conflicts, nor have any been sufficiently attributed to the sponsorship of specific countries. Other than the warfare paradigm, the international community appears to have no commonly-accepted framework for managing cyber threats or incidents that impact national security. Further, there is no international agreement that mandates each country have a minimum cyber incident response capability so that cooperation can be provided. There is no single organization that coordinates multinational cyber incident response efforts.

In 2009 an American Bar Association report noted that "the single greatest difficulty encountered thus far in the development of a legal response [to the national security cyber threat] lies in the transnational nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace."[172] Other legal and technical experts may disagree on the need for such legal structures. It is therefore important to investigate this issue in depth, analyzing and comparing various international legal approaches, and incorporating insight and critique by operational experts who understand the technology and business realities.

When faced with global threats or with international threats to a certain geographical region, nations have developed a variety of legal frameworks for cooperation, guidance, and accountability. International legal frameworks help manage global threats such as pandemics and the proliferation of nuclear weapons. Similarly, legal structures address international or regional threats like maritime piracy and environmental pollution. International humanitarian law and human rights law hold nations and individuals accountable for certain internationally wrongful acts. Before creating new constructs and laws, existing legal frameworks should be assessed to determine their applicability to global and international cyber threats. The following tables provide examples of two comparisons which may be investigated.

172 Paul Rosenzweig, Workshop Rapporteur, *National Security Threats in Cyberspace*, Post-Workshop Report, American Bar Association Standing Committee on Law and National Security & The National Strategy Forum (Sept. 2009), http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf.

TABLE ONE

GLOBAL ALERT AND RESPONSE	CYBER COMPARISON
Concerns about the spread of cholera and other epidemics in the mid-to-late 1800s led to international movements that have evolved into the United Nations World Health Organization ('WHO'). Today the WHO establishes norms and standards, provides technical support to improve the health infrastructure within member states, delineates policy guidelines based on scientific and technical evidence, and coordinates international watch and warning and response efforts to minimize the spread of infectious diseases. The WHO maintains a Global Outbreak Alert and Response Network to share intelligence and manage response to incidents. Incident management may include tracking the incident's origins and critical decisions of responders; providing logistics support and access to necessary equipment and supplies; coordinating international response teams; and organizing lines of communication and standardizing public messaging. The WHO's International Health Regulations ('IHR') were first established in 1969. The IHR are legally binding on almost 200 countries. In the most recent redraft of 2005, the IHR require minimum levels of national public health capabilities, mandate incident reporting by member states, and are applicable not only to disease outbreaks but to any serious public health emergency no matter the cause (e.g., chemical leaks or spills and nuclear melt-downs).	Many countries, private businesses, and organizations have watch and warning capabilities for cyber security. Companies such as those who run the Internet backbone have operations centers that constantly monitor global communications traffic. These companies communicate with each other as necessary to manage incidents affecting their networks. Depending on the severity or complexity of an incident, they may also communicate with national or organizational Computer Emergency Readiness Teams ('CERT'). Some governments require private sector reporting of cyber incidents, but other countries instead pursue "public-private partnerships" (cooperative agreements for information sharing and response coordination). For those countries that mandate incident reporting, the laws vary in both definition and scope; countries differ in defining what type of incident must be reported, and the reporting mandate may only apply to certain industries such as telecommunications companies. There is no international, commonly-enforced standard for incident reporting. There is no global organization that mandates minimum levels of national cyber incident response capabilities. While there is no cyber equivalent to the IHR, the closest analogy to the WHO may be the Forum of Incident Response and Security Teams ('FIRST'), whose members include government incident response teams as well as experts from industry and academia. However, as a voluntary, fee-for-membership organization not originating from within an organization such as the United Nations, FIRST is significantly different from the WHO.

TABLE TWO

STATE RESPONSIBILITY	CYBER COMPARISON
Non-state actors are a growing threat to national security. State responsibility for internationally wrongful acts committed by non-state actors is an evolving area of law. In *Nicaragua v. United States*, the International Court of Justice found that in order for a state to be responsible for human rights violations perpetrated by non-state actors, the state must have had "effective control" of the perpetrators. Under this standard, a nation may finance, train, equip, and organize the non-state actors, and yet still not meet the "effective control" test. The Appeals Court of the International Criminal Court for the Former Yugoslavia in the *Tadic* case presented a different standard. The court held, inter alia, that when the non-state actors were not organized militarily, state responsibility for the non-state actors' humanitarian violations existed when the state had "overall control" of the non-state actors. Such "overall control" may be shown by the state's financing, training, or equipping of the perpetrators and by coordinating or planning their actions. Another international law guideline developed after the terrorist attacks against the United States in September 2001. The United States held Afghanistan responsible for merely harboring and supporting al Qaeda – far below the standard of "effective control" or even "overall control." The United Nations Security Council, NATO, and the Organization of American States sanctioned this approach; numerous international law experts also supported this position.	In recent years, of the major international cyber incidents that were made public, most were conducted by non-state actors. Because of the anonymous nature of the Internet, it is difficult to obtain high levels of confidence in attribution of an act to an individual or group, or to show that a nation state sponsored a cyber attack conducted by non-state actors. Even if such proof is discovered, the standards of "effective control," "overall control," or "harboring and supporting" may not be applicable to cyber incidents. The state responsibility standards adhere to internationally wrongful acts which traditionally include genocide, violations of law applicable to armed conflicts, and crimes against humanity. These wrongful acts do not easily correlate to acts performed during cyber incidents which significantly damage a national economy or other critical infrastructure asset. Once "cyber incident-related" activities are identified as internationally wrongful acts, then the state responsibility standards may be analogized.

These examples are not meant as ideals of what is needed in the cyber realm; rather, they are examples of approaches and perspectives that may be investigated. Policymakers can learn much, not only from the processes and development of these international constructs, but also from the years of critique on how to improve such frameworks.

Cyber law literature is currently weighted with cyber war and traditional criminal law analyses. However, paradigms of criminal law and international law (state-on-state

aggression, armed conflicts) may not provide enough perspective regarding state responsibility for cyber incidents. To properly mitigate and manage national and international cyber security threats, additional perspectives and constructs may be needed. The goal of this presentation and whitepaper is to encourage analysts to look beyond the perspectives of warfare and crime, and to suggest that before new constructs or new laws are created, existing legal frameworks should be assessed to determine their appropriateness for managing global and international cyber threats.

CYBERSECURITY REGULATION: USING ANALOGIES TO DEVELOP FRAMEWORKS FOR REGULATION[173]

Julie J. C. H. Ryan[174], Daniel J. Ryan[175], Eneken Tikk[176]

Abstract

Cyberspace has been referred to as "wild, wild west" by a number of authors over past 20 years. The international cyber incidents witnessed by the international community in the past three years have awaked the international discussion on the regulation of the domain that is developing into a self-standing dimension of our daily life, national security and warfare. For the purposes of this article, cyberspace may be regarded as one of the great "commons". The purpose of taking this perspective is to evaluate the usefulness of the commons regulation analogy for resolving some of the issues nations and international community faces in regard to cyber security, and for guiding the development of a regulatory framework for cyberspace.

INTRODUCTION

A variety of analogies and metaphors have been proposed as aids for thinking about cyberspace and regulation of human behavior in cyberspace. For example, we talk about the information superhighway as a way of understanding traffic of

173 Opinions expressed in this paper are those of the authors and do not represent positions of George Washington University, or of the Information Resources Management College, the National Defense University, the Department of Defense, or the United States Government, or of the Cooperative Cyber Defence Centre of Excellence, the Government of Estonia, or NATO.
The following students performed research that informed our progress in writing this paper: James Allen, William Biggs, Joseph Bober, Earl Britt, Cynthia D. Brown, John Coller, Charles F. Hall, Daniel Jennings, Brenda Magente, Mark S. Mistal, Bruce W. Morris, Debora L. Nissenbaum, David B. Odom, Michael F. Pennock, Linda Snowden-Peninger, Timothy Potz, David W. Stickley, Linda Suppan, Stephen B. Sznajder, Uzill Weaver, and Howard G. W. Whyte.

174 Julie J. C. H. Ryan, Department of Engineering Management and System Engineering, School of Engineering and Applied Science, The George Washington University, Washington, D. C. 20052, USA, jjchryan@gwu.edu

175 Daniel J. Ryan, Department of Information Operations & Information Assurance, Information Resources Management College, National Defense University, Washington, D. C. 20319, USA, ryand@ndu.edu

176 Eneken Tikk, Legal Advisor / Head of Legal and Policy Branch, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, eneken.tikk@mil.ee

information across the World Wide Web. Even calling the Internet a "web" invokes a metaphor. Alternatively, cyberspace may be thought of as a *res communis*, a commons.[177] We know that men have been concerned with the regulation of the use of commonly owned resources since the dawn of history, and it is easy to imagine that such concerns predate historical records, since use of natural resources in prehistoric times must have required attention to who could use hunting and gathering territories, for example. Certainly the Greeks as early as the fifth century BCE were familiar with the problem. In 431 BCE, Thucydides wrote, "[T]hey devote a very small fraction of time to the consideration of any public object, most of it to the prosecution of their own objects. Meanwhile each fancies that no harm will come to his neglect, that it is the business of somebody else to look after this or that for him; and so, by the same notion being entertained by all separately, the common cause imperceptibly decays."[178] Eighty years later, Aristotle wrote, "That all persons call the same thing mine in the sense in which each does so may be a fine thing, but it is impracticable; or if the words are taken in the other sense, such a unity in no way conduces to harmony. And there is another objection to the proposal. For that which is common to the greatest number has the least care bestowed upon it. Each one thinks chiefly of his own, hardly at all of the common interest; and only when he is himself concerned as an individual. For besides other considerations, everybody is more inclined to neglect the duty to which he expects another to fulfill; as in families many attendants are often less useful than a few."[179] Two millennia later, in 1833, William Forster Lloyd, then Drummond Professor of political economy at Oxford, in attempting to refute Adam Smith's notion of a felicitous "invisible hand" that converted selfish behavior into common prosperity, coined the term "commons" to describe depletion of commonly owned resources through overuse due to maximization of short-term individual selfish interests.[180] In 1968, Garrett Hardin borrowed the term in his now-famous paper, "The Tragedy of the Commons."[181] Hardin's use of the term "tragedy" harkens back to the Greeks

177 See Peter Levine (Fall, 2001) Civic Renewal and the Commons of Cyberspace, *National Civic Review*, Vol. 90, No. 3. See also Dan Hunter (2003) Cyberspace as Place and the Tragedy of the Anticommons, 91 Cal. L. Rev. 439.

178 Thucydides, *History of the Peloponnesian War*, Book I, Sec. 141; translated by Richard Crawley (London: J. M. Dent & Sons; New York: E. P. Dutton & Co., 1910). Online at http://people.ucalgary.ca/~vandersp/Courses/texts/thucydi1.html#CH.V. Cited in Denmark and Mulvenon, p 44 n. 21. See also http://en.wikipedia.org/wiki/Tragedy_of_the_commons#References_to_the_Greek_classics.

179 Aristotle, *Politics*, Book II, Chapter III, 1261b; translated by Benjamin Jowett as The Politics of Aristotle: Translated into English with Introduction, Marginal Analysis, Essays, Notes and Indices (Oxford: Clarendon Press, 1885), Vol. 1 of 2. Online at http://classics.mit.edu/Aristotle/politics.2.two.html. Cited in Denmark and Mulvenon, p 44 n. 21. See also http://en.wikipedia.org/wiki/Tragedy_of_the_commons#References_to_the_Greek_classics.

180 *W. F. Lloyd on the Checks to Population. Population and Development Review*, Vol. 6, No. 3 (Sep., 1980), pp. 473-496. http://www.jstor.org/stable/1972412

181 "The Tragedy of the Commons," Garrett Hardin, Science, 162(1968):1243-1248.

notion of tragedy: "The essence of dramatic tragedy is not unhappiness. It resides in the solemnity of the remorseless working of things."[182]

Today there are many commons that may require regulatory attention. Grazing land may be publically owned, as in Lloyd's original exposition. Public facilities such as government buildings and land, parks, navigable waterways and the continental shelf may be considered commons. That body of knowledge residing in the public domain or the results of science and technology sponsored by the government may be thought of as commons. Oil, minerals, timber, and other resources found on or beneath public lands or under the surface of the sea comprise natural commons. The open seas, the atmosphere, outer space above the atmosphere, the Arctic icecap, the Antarctic continent, and the electromagnetic spectrum are resources owned in common by the citizens of the world.

States may try and control that portion of such commons over which they exercise jurisdiction, or may enter into international treaties for regulation of some commons or parts of commons. In other cases, individual entrepreneurs, private non-governmental organizations (NGOs) or corporations may seek to control and exploit parts of some commons for specific purposes or material gain.

Beginning with four nodes in 1969,[183] the wide area network-of-networks we call cyberspace[184] has grown and spread to become a commons, a critical infrastructure that is pervasive and upon which societies worldwide have become dependent for commerce, recreation, communication, delivery of government services, research, education and a host of other activities. United States President George W. Bush has said, "The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace."[185] Cyberspace is our most recent commons,[186] but the problem of regulating human behavior in the use of commons is not, so we should be able to draw upon the lessons we have learned as we regulated behavior in other, earlier commons that can inform and facilitate the development of effective and efficient regulatory architectures for regulation of cyberspace.

182 Alfred North Whitehead, *Science and the Modern World* (Mentor, New York, 1948), p. 17. Cited in Hardin.
183 http://www.davesite.com/webstation/net-history.shtml
184 The term "cyberspace" was coined by the science fiction author William Gibson in his 1982 cyberpunk story "Burning Chrome."
185 http://georgewbush-whitehouse.archives.gov/pcipb/letter.pdf
186 Exactly when the cyberspace commons began depends upon the definition of cyberspace. The Internet arguably dates from December, 1969, but the use of technologies to facilitate communications and commerce arose much earlier. See Tom Standage (1998) *The Victorian Internet*. New York: Walker & Company. www.walkerbooks.com.

This is an ambitious undertaking. The best-known commons – the sea, the atmosphere, outer space, and Antarctica – have evolved comprehensive regulatory frameworks based on customary international law and treaties. Thus we have:

- The laws of the sea (maritime commons)
- Regulation of air traffic control (atmosphere commons)
- The Antarctic Treaties (Antarctic commons)
- Treaties controlling the use of outer space (extra-atmospheric commons)

Other regulatory frameworks may provide ways of better understanding how regulatory schema might evolve for cyberspace. These include, but are not limited to:

- The Laws of Armed Conflict (LOAC, or International Humanitarian Law)
- Environmental law
- Public health, epidemiological control and The World Health Organization (WHO)
- The World Intellectual Property Organization (WIPO) and control of intangible property
- Control of the electromagnetic spectrum
- Control of international commerce
- Water use regulation for non-tidal water
- Critical Infrastructure Protection (CIP) laws and regulations

We have the beginnings of a regulatory framework for cyberspace, including:

- Internet governance by NGOs[187]
- Cybercrime statutes at national levels[188]
- The European Cybercrime Convention[189]

But human occupation and use of cyberspace is relatively recent, and a comprehensive framework for regulation in cyberspace is still evolving. Each of the

187 See Milton Mueller (2004) *Ruling the Root: Internet Governance and the Taming of Cyberspace* . Cambridge, MA: MIT Press. See also http://www.ietf.org/ and http://www.icann.org/.
188 See, for example, http://www.law.cornell.edu/uscode/18/1030.html.
189 See http://conventions.coe.int/Treaty/EN/Treaties/HTML/185.htm . Also, http://epic.org/privacy/intl/ccc.html.

other commons and analogies may provide similes and metaphors that can inform and guide the evolution of rules for regulating human behavior in cyberspace.

Still, we must acknowledge at the outset that no analogy is perfect, and metaphors, while they can vividly illuminate areas of concern, can also mislead and confuse, even as they inform and guide. Therefore, as we explore these analogies and metaphors to glean guidance relevant to regulation of human behavior in cyberspace, we will maintain caution to avoid the fog of policy.

We will begin with the best known commons: the seas, the atmosphere, outer space and Antarctica.

THE LAW OF THE SEA

The seas constitute a commons that mankind has used for thousands of years for commerce, communication, and exploitation of the animals and plants it contains and of the minerals beneath the sea floors. Control of the use of the seas and its vast wealth is increasingly important as world population grows and per capita natural resources decline, both on- and off-shore.

Control of the seas has been contentious among European powers for well over five hundred years. Norway and Denmark claimed sovereignty over the Arctic Ocean (*Mare Septentrionale*) and Denmark and Sweden exercised control over the Baltic (*Dominium maris Baltici*).[190] Pope Alexander Borgia, to control access to the newly discovered Americas, arrogantly divided power over the ocean commons between Spain and Portugal in 1493, with a demarcation line 100 leagues west of the Azores.[191] All newly discovered lands west of the line were to be under Spanish control and all lands east of the line went to Portugal, and no other countries were allowed to sail to and trade with the new lands (*mare clausum*).[192] In the 17th century, Great Britain claimed control over a large area of the seas (*Oceanus Britannicus*). Needless to say, such claims led to much tension and outright conflict as the European powers tried to preserve the use of the sea to their country's military forces and commercial traders, while denying the use of sea lanes to their enemies.

In 1609, Hugo Grotius published his famous book *Mare Liberum*, promoting the principle of freedom of the seas. He argued that the seas were for the use of all, not subject to the control of a few strong nations. States that had coastlines were to

190 B. J. Theutenberg (1984) The Evolution of the Law of the Sea. Dublin: Tycooly International Publishing Limited, p. 1.
191 On June 7, 1494, the Treaty of Tordesillas moved the line to 370 leagues west of the Cape Verde islands, reserving Brazil to the Portugese and the rest of the New World to the Spanish. *Ibid.*
192 Theutenberg (1984).

be allowed control of a narrow strip of water along their coasts (territorial waters). Originally, territorial waters were conceived to be the part of the ocean that could be defended from shore – hence, one cannon shot in width. This distance was arbitrarily extended to 3 nautical miles (6 km) by several nations, including the United States, Great Britain and France. Iceland claimed two nautical miles, Norway four and Spain six. Late in the twentieth century, those claims were expanded by many nations to twelve nautical miles.[193]

The League of Nations made an attempt to develop a Law of the Sea Treaty in 1930, but the effort failed. In general, that part of the ocean that was not included in the territorial waters of some nation was available for use by anyone with a vessel (*usus publicus*), making international waters a commons. This principle was codified in the 1958 Geneva Convention on the High Seas.[194]

Claims to the right to control natural resources in and under the waters above the continental shelves adjacent to the land areas of nations were asserted by the United Kingdom and Venezuela, a claim espoused by the United States in 1945.[195] Control of the continental shelf was eventually codified in the Geneva Convention on the Continental Shelf in 1958.[196] The Third Conference on the Law of the Sea aimed to develop a comprehensive framework for regulating the utilization of the oceans and the seafloor. After fourteen years of work by 150 nations, the Conference adopted the United Nations Convention on the Law of the Sea Convention (UNCLOS) on December 10, 1982 at Montego Bay, Jamaica. UNCLOS codified the norms that had evolved over many years for controlling the use of the seas and the natural resources beneath the seabed. The Convention addressed for the first time environmental preservation and protection and deep ocean floor resources. UNCLOS was signed quickly by one hundred and nineteen states and finally came into force with ratification by 60 nations on November 16, 1994.[197] The UN says, "It is a complex and broad-ranging formulation of international law that seeks to regulate the world's oceans for the benefit of mankind.[198]"

193 While it is foreseeable that countries have different "cyber perimeter defense" capabilities, the principle of effective control could stress the responsibility of nation states to design information society so that it has the required level of security built in.
194 Theutenberg (1984).
195 *Department of State Bulletin*, September 30, 1945, p. 485.
196 Theutenberg, p. 2.
197 Conflicting interests, particularly regarding regulation of the use of deep seabeds, delayed the ratification of the Convention for many years after its signing in 1982. Eventually, in 1994, an agreement was reached on implementation of Part XI of the Convention, and the necessary 60 ratifications were attained. www.eoearth.org/article/United_Nations_Convention_on_Law_of_the_Sea_(UNCLOS),_1982.
198 United Nations Convention on the Law of the Sea of 10 December 1982- Overview and full text. (last updated January 8, 2010), Chapter 1 -3.

Today, the seas are divided into zones for purposes of regulation. The so-called "territorial waters" within twelve miles of the mean-low-water line of a coastal state are under the direct sovereign control of the state.[199] The air above these waters and the seabed below are also within the sovereign control of the state. Congruent with the territorial waters or perhaps as far as twenty-four miles beyond the mean-low-water line, a "contiguous zone" may allow a nation to exercise limited enforcements of customs, fiscal or immigration policies or sanitary laws. Finally, an exclusive economic zone is deemed to extend out to 200 nautical miles, and within that zone a costal nation can exercise control over all of the economic resources found there – living and mineral – and can regulate pollution of the waters within the zone. It may not, however, prohibit transiting of those waters by vessels in compliance with laws and regulations adopted by the costal nation in accordance with UN conventions.

The oceans outside of national jurisdiction are called variously "international waters", the "high seas", or *Mare Liberum*. Ships sailing on the high seas fall under the jurisdiction of their country of registry. The use of the high seas is subject to UNCLOS, especially Articles XII-XIV, and may also be subject to other global treaties and conventions, regional agreements such as those included in the Regional Seas Program of the United Nations Environment Programme,[200] or specific agreements for the use of certain bodies of water, e.g. the Helsinki Convertion on the Protection of the Marine Environment of the Baltic Sea.[201]

The seas and cyberspace share several important characteristics. Both are expansive domains in which humans can operate using specially designed and developed technologies. Neither is wholly contained within the sovereign territory of a single nation or small group of nations, and many nations profit from more or less simultaneous access to and free transit across these domains. Both require human investment of scarce resources to realize their potential, and both share analogous risks from property appropriation to criminal activity to warfare.

On the other hand, cyberspace, unlike the ocean, is mostly[202] manmade, and requires near-continuous human attention and support to remain functional. The seas have more-or-less well-defined boundaries related to topographically defined jurisdictions in physical space, while cyberspace has only weak connectivity to

199 If an overlap with another nation's territorial waters would occur, the boundary is taken to be the median points between the state's baseline mean-low-waters.
200 www.unep.org.
201 www.helcom.fi/Convention.
202 Certain portions of cyberspace use paths through the atmosphere and outer space for communications.

physical space.[203] And the technologies for using and exploiting cyberspace are evolving more rapidly today than those we use to take advantage of the oceans and the treasures beneath them.

AIR TRAFFIC CONTROL

One hundred years ago, airspace was mostly uncontrolled, as cyberspace is today. If you wanted to fly, you built or bought an airplane, studied (hopefully) how to take off and land and how to steer when airborne, and off you went. Neither flying nor airfields were subject to regulation. Today, flying, whether for recreation or for commercial purposes, is highly regulated, from licensing of pilots to safety of airplanes to use of airfields to transnational travel and commerce. How did this massive and pervasive regulatory structure evolve, and what lessons does it offer to us as we consider regulation of cyberspace?

Air traffic control rules are used to separate aircraft to prevent collisions and to organize and facilitate the flow of air traffic through the atmospheric commons. Some airspace is controlled (over national territories) and some is not (over international waters or Antarctica). Air traffic control activities may involve instructions to pilots that they are required to obey, or may merely provide information to pilots that does not involve mandatory instructions.

Heavier that air human flight began on December 17, 1903, when Orville and Wilber Wright made the first controlled, powered and sustained fixed-wing aircraft flight. In 1910, the first conference on regulation of the use of aircraft was held in Paris. By 1919, airplane use had grown to the point that international regulation was deemed necessary, and the International Commission for Air Navigation (ICAN) was created to develop rules for air traffic control. A Convention of forty-three articles, incorporating all of the principles discussed at the 1910 conference, was established to deal with technical, operational and organizational aspects of civil aviation.[204] The United States, still somewhat geographically isolated (at least in terms of air navigation), did not sign the ICAN Convention, developing its own rules somewhat later after the passage of the Air Commerce Act (ACA) of 1926. The ACA authorized the Department of Commerce to develop rules for air navigation, protection and identification of aircraft operating within the United States.

Early rules under the ACA in the United States focused on individual airport operations, but by 1935, the volume of air traffic had increased to a level that led

203 It is true that every computer, server, workstation and wire has some location in physical space, but these are largely transparent to transactions across cyberspace.
204 www.icao.int//cgi/goto_m.pl?icao/en/hist/history01.htm.

to coordination of traffic among airports. In December of 1935, the first air traffic control center opened at Newark, New Jersey. Additional centers at Chicago and Cleveland opened the next year. In July, 1936, en route air traffic control became a federal responsibility in the United States. In 1941, congress created the Civil Aeronautics Administration (CAA) to operate the air traffic control system. There were 155 air traffic control towers in the United States by 1944. By 1952, local radar was operational in the air traffic control system, and by 1956, and order for long-range radars for use in air traffic control was placed.

By the 1940's the volume of transnational air traffic to and from the United States made it clear that the United States and other nations could not continue to evolve independent and different air traffic control systems. On December 7, 1944, the International Civil Aviation Convention (commonly referred to as the Chicago Convention) was signed by 52 countries to create a common framework for control and regulation of air traffic. The 26th ratification occurred March 5, 1947, and the Convention became effective April 4, 1947. Since then, the Convention has been revised eight times to keep pace with the evolution of aircraft and aircraft control technologies and the increasing density of international air traffic. Today, air traffic control rules are managed by a United Nations Specialized Agency, the International Civil Aviation Organization (ICAO).[205] One hundred and ninety (190) states[206] worldwide follow ICAO rules in managing civil aviation within and between their national airspaces.

Like the seas, the atmosphere is divided into regions subject to different regulatory schemes. Some airspace is controlled – subject to Air Traffic Control regulations – and some is uncontrolled. The busy areas around airports are controlled to prevent collisions among planes. Specific rules apply to planes flying at cruising altitudes to expedite and maintain the orderly flow of air traffic, especially with regard to Instrument Flight Rules (IFR). Security is also important and certain areas are designated Air Defense Identification Zones (ADIZ). ADIZ are no fly zones with very strict rules. Altogether there are seven classes of airspace defined by the ICAO. They are designated A to G and ATC flight regulations take effect at E and progress in descending alphabetical order. Classes F and G are uncontrolled airspace. Not all countries use all seven classes of airspace in regulating air traffic above their territories.[207] Some airspace may be designated Special Use Airspace and is off limits for non-military aircraft. Special Use Airspace includes Prohibited Areas, Restricted Areas, Alert Areas, Warning Areas, and Military Operations Areas.[208]

205 www.icao.int.
206 www.icao.int/cgi/statesDB4.pl?en.
207 http://www.dicksmithflyer.com.au/airspace_categories.php.
208 http://quest.arc.nasa.gov/aero/virtual/demo/navigation/youDecide/airspace.html.

Both the atmosphere and cyberspace are extensive domains within which humans, using appropriate technology, can operate. Both are international in scope and use, with some areas within existing national jurisdictions and some areas outside of any national jurisdiction. Both have traffic flows that need to be controlled to facilitate transiting the domain.

While airspace is tightly connected to national jurisdictions and traffic is under the control of a specific jurisdiction when above a national jurisdiction, traffic in cyberspace is much less subject to such controls. Air traffic is tightly monitored and directed by the Air Traffic Control system; packets in cyberspace take unpredictable paths dictated by network routing protocols that can change dynamically in response to loading in ways that are not controlled or controllable by either the user or the nations the traffic paths traverse. Both planes and passengers are identified and tracked when they use airspace, but authentication and attribution of users of cyberspace is often impossible.

This analogy of cyberspace to the atmospheric commons leaves hope for those who argue that cyberspace has grown way over the head of the regulators. One could see the first wave of cyber domain regulation occur in early 90's. A revision of the original approaches has been undertaken in most countries during 2000-2005, but the occurrence of the Estonian case in 2007 clearly indicated that national homework regarding regulation of behavior in cyberspace is nowhere near to "done". Various entities and organizations are focusing on security standards for cyberspace – for example, IANA and ICANN deal with Internet assigned names and numbers or the domain name system, the European union has started a comprehensive information society development coordination effort, and the Council of Europe has contributed to the uniformity of criminal law in the field.

Thus, it would be unfair to conclude that from the regulatory perspective, the Internet is a sum zero. It is rather that some aspects of this traffic (such as national security emergency vehicles and "cyber tanks") have been left aside while others such "cargo flights" (business uses of the Internet) and some charter flights (e.g. personal data protection, consumer rights) have been heavily regulated. Furthermore, often regulation of the cyberspace domain has occurred on the national level and is thus subject to sovereignty ramifications. Private jets in the Internet are fairly easy to operate as the end users' rights have flourished under the regulation ruled by the human rights paradigm.

OUTER SPACE

Man began to explore and exploit the outer space commons just over a half

century ago: orbiting satellites, space stations and space laboratories, sending men to the moon and back, and launching deep-space exploration vehicles like Voyager 1 and 2.[209] Early efforts were undoubtedly driven by the competition between the United States and the, then, Soviet Union,[210] but with the first moon landing Neil Armstrong, saying "That's one small step for (a) man, one giant leap for mankind," made it clear that outer space is not the territory of one or a few countries, but the common territory of all.[211] "Outer space as a common territory beyond national jurisdiction is a "global commons" *par excellence*. Security must therefore be common, cooperative security, based on the rule of law and respect for international space law in the interest of all states and mankind as a whole."[212]

With the space race fully underway, the United Nations adopted its "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space" in 1963.[213] The nine legal principles are:

1) The exploration and use of outer space shall be carried on for the benefit and in the interests of all mankind.

2) Outer space and celestial bodies are free for exploration and use by all States on a basis of equality and in accordance with international law.

3) Outer space and celestial bodies are not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.

4) The activities of States in the exploration and use of outer space shall be carried on in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding.

5) States bear international responsibility for national activities in outer space, whether carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried on in conformity with the principles set forth in the present Declaration. The activities of non-governmental entities in outer space shall require authorization and

209 National Aeronautics and Space Administration, Jet Propulsion Laboratory, Frequently Asked Questions, http://voyager.jpl.nasa.gov/faq.html.
210 On October 4, 1957, the then Soviet Union launched its Sputnik satellite, the first successful orbiting of a man-made satellite, and ushered in the Space Age.
211 Jones, Eric M. (1995) *One Small Step.* NASA's Apollo 11 Lunar Surface Journal. http://history.nasa.gov/alsj/a11/a11.step.html
212 Detlev Wolter (2003) *Common Security in Outer Space and International Law: A European Perspective,* p. 4.
213 http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_18_1962.html.

continuing supervision by the State concerned. When activities are carried on in outer space by an international organization, responsibility for compliance with the principles set forth in this Declaration shall be borne by the international organization and by the States participating in it.

6) In the exploration and use of outer space, States shall be guided by the principle of co-operation and mutual assistance and shall conduct all their activities in outer space with due regard for the corresponding interests of other States. If a State has reason to believe that an outer space activity or experiment planned by it or its nationals would cause potentially harmful interference with activities of other States in the peaceful exploration and use of outer space, it shall undertake appropriate international consultations before proceeding with any such activity or experiment. A State which has reason to believe that an outer space activity or experiment planned by another State would cause potentially harmful interference with activities in the peaceful exploration and use of outer space may request consultation concerning the activity or experiment.

7) The State on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object, and any personnel thereon, while in outer space. Ownership of objects launched into outer space, and of their component parts, is not affected by their passage through outer space or by their return to the earth. Such objects or component parts found beyond the limits of the State of registry shall be returned to that State, which shall furnish identifying data upon request prior to return.

8) Each State which launches or procures the launching of an object into outer space, and each State from whose territory or facility an object is launched, is internationally liable for damage to a foreign State or to its natural or juridical persons by such object or its component parts on the earth, in air space, or in outer space.

9) States shall regard astronauts as envoys of mankind in outer space, and shall render to them all possible assistance in the event of accident, distress, or emergency landing on the territory of a foreign State or on the high seas. Astronauts who make such a landing shall be safely and promptly returned to the State of registry of their space vehicle.[214]

The Declaration has since been supplemented by three resolutions laying down

214 *Ibid.*

the legal principles applicable to the exploration and exploitation of outer space,[215] the "Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries,"[216] and five treaties and agreements governing the use of space and space-related activities.[217] These treaties, agreements and principles are collectively known as the "United Nations Treaties and Principles in Outer Space," which make access to and use of space available, limit the use of space to peaceful purposes (especially avoiding the weaponizing of space with nuclear[218] and other weapons of mass destruction, although not all weapons are banned from space, e.g. lasers or kinetic weapons), and fostering cooperation for the protection and recovery of astronauts. All of this was accomplished in spite of the fact that after more than twenty years of trying, there is still no accepted legal definition of "outer space."

In addition to United Nations Treaties and Principles in Outer Space efforts to regulate the use of outer space, other treaties and agreements offer additional regulations. Through the Convention of the International Telecommunications Union, the United Nations International Telecommunication Union "has coordinated the shared global use of the radio spectrum, promoted international

215 The Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting (resolution 37/92 of 10 December 1982), http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_37_0092.html; The Principles Relating to Remote Sensing of the Earth from Outer Space (resolution 41/65 of 3 December 1986), http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_41_0065.html; The Principles Relevant to the Use of Nuclear Power Sources in Outer Space (resolution 47/68 of 14 December 1992), http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_47_0068.html.

216 http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_51_0122.html.

217 The "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies" (the "Outer Space Treaty", adopted by the General Assembly in its resolution 2222 (XXI)), entered into force on 10 October 1967, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_21_2222.html; the "Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space" (the "Rescue Agreement", adopted by the General Assembly in its resolution 2345 (XXII)), entered into force on 3 December 1968, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_22_2345.html; the "Convention on International Liability for Damage Caused by Space Objects" (the "Liability Convention", adopted by the General Assembly in its resolution 2777 (XXVI)), entered into force on 1 September 1972, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_26_2777.html; the "Convention on Registration of Objects Launched into Outer Space" (the "Registration Convention", adopted by the General Assembly in its resolution 3235 (XXIX)), opened for signature on 14 January 1975, entered into force on 15 September 1976, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_29_3235.html; and the "Agreement Governing the Activities of States on the Moon and Other Celestial Bodies" (the "Moon Agreement", adopted by the General Assembly in its resolution 34/68), entered into force on 11 July 1984, http://www.oosa.unvienna.org/oosa/en/SpaceLaw/gares/html/gares_34_0068.html.

218 Although nuclear weapons are banned, it is recognized that some uses of nuclear power are needed in space, the Treaties and Principles provide for safety in its use, mitigation of risks, and liability for states that fail to control the nuclear power or its sources. http://www.unoosa.org/oosa/SpaceLaw/nps.html.

cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world, established the worldwide standards that foster seamless interconnection of a vast range of communications systems and addressed the global challenges of our times, such as mitigating climate change and strengthening cybersecurity."[219] The 1963 Partial Test Ban Treaty[220] prohibits the explosion of nuclear bombs in outer space. Multilateral and bilateral agreements and treaties, "such as the Convention of the European Space Agency in 1975, Arabsat in 1976, and EUMETSAT in 1983,"[221] may regulate the use of space among the parties to those agreements and treaties. Voluntary *schema* include the Missile Technology Control Regime (1987),[222] the Committee on the Peaceful Uses of Outer Space ("COPUOS"),[223] and the Global Exploration Strategy.[224] And, of course, Customary International Law applies.

Cyberspace and Outer Space share some interesting similarities. The use and exploitation of each is heavily technology-dependent. The inherent nature of each is only loosely related to traditional notions of territorial sovereignty. Although every computer, server and wire is located in some place subject to other regulatory frameworks, the paths by which packets travel across the Internet are largely beyond the control of the user and may pass through many different sovereign jurisdictions in route from sender to recipient. Spacecraft and satellites in orbit pass above many different sovereign jurisdictions and cannot avoid doing so, the laws of celestial mechanics being as they are. Thus, the notions of territorial control that apply well in the laws of the sea and the regulation of international air travel, do not apply well to outer space or cyberspace. If nations were allowed to exercise sovereign control over the use of outer space in the same way they exercise sovereign control of air traffic in the skies above their territories, it might be practically impossible to explore and use space at all. The same may apply to cyberspace.

Of course, despite their similarities, outer space and cyberspace are inherently different. One is real; the other virtual. Although cyberspace requires a physical medium, it exists within and among the components that comprise that medium, and as those components come and go, cyberspace expands and contracts. Cyberspace is polymorphic in ways that outer space is not. Disconnect the components and cyberspace evaporates; outer space is here to stay. These differences mean that, while a framework of principles, agreements and treaties

219 http://www.itu.int/net/about/index.aspx.
220 http://nuclearfiles.org/menu/library/treaties/partial-test-ban/trty_partial-test-ban_1963-10-10.htm.
221 Johnathan F. Galloway (2008) *Conference on Space and Telecommunications Law: Revolution and Evolution in the Law of Outer Space*, 87 Neb. L. Rev. 516.
222 http://www.mtcr.info/english/index.html. Cited in 87 Neb. L. Rev. 516.
223 http://www.oosa.unvienna.org/oosa/COPUOS/copuos.html. Cited in 87 Neb. L. Rev. 516.
224 http://www.nasa.gov/pdf/178109main_ges_framework.pdf. Cited in 87 Neb. L. Rev. 516.

may well serve to regulate behavior in cyberspace, they may not be the same principles, agreements and treaties that have evolved to control behavior in outer space. Professor Lessig[225] had it right when he told us that code *is* law, that the architecture of a place limits and enables the rules we can expect to work well in controlling behavior in those places. Differences in architectures require differences in rules of behavior. The trick is to use what is usable in common, without trying to use what is not.

MANAGING ANTARCTICA

We explore and use cyberspace from the comfort of our homes and offices. The seas, the air and outer space require that we create vessels that can sustain friendly environments around us as we traverse, use and exploit their resources. In some ways the most difficult of the great commons for humans to explore and use is the intensely cold and inhospitable Antarctic continent.

In 1773, James Cook circumnavigated Antarctica. Exploration of the Earth south of the Antarctic Circle began in earnest about 1820, when Russian, British, French and American teams began to visit the icebound region. February 7, 1821, saw the first landing on the continent by the American sealer Captain John Davis, the first of many visits by sealers and whalers. Later that year, ten British sailors and one officer were marooned and unwillingly spent the winter, the first winter-over by humans. By 1840, Antarctica was known to be a continent. In 1898, the first scientific expedition wintered over, also unwillingly. In 1902, Captain Robert Falcon Scott, with Ernest Shackleton and Edward Wilson, tried unsuccessfully to reach the South Pole. In 1907-9, Shackleton tried again and got within 156 km of the Pole. In 1909, Douglas Mawson reached the South magnetic pole, and, finally, in 1911, the Norwegian Roald Amundsen led a five-man team to the Pole itself.[226]

> Fortunately, scientific interests rather than political, economic, or military concerns dominated the expeditions sent to Antarctica after World War II. Fortunately, too, international scientific associations were able to work out arrangements for effective cooperation. In 1956 and 1957, for example, American meteorologists "wintered over" at the Soviet post Mirnyy, while Soviet meteorologists "wintered over" at Little America. These cooperative activities culminated in the International Geophysical Year of 1957-1958 (IGY), a joint scientific effort by 12 nations -- Argentina, Australia, Belgium, Chile, France, Japan, New Zealand, Norway, South Africa, the Soviet Union, the United Kingdom, and the United States -- to conduct studies of the Earth and its

225 Lawrence Lessig (1999) Commentary: The Law of the Horse: What Cyberlaw Might Teach. 113 Harv. L. Rev. 501. http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF.

226 http://www.coolantarctica.com/Antarctica%20fact%20file/History/exploration%20and%20history.htm.

cosmic environment.[227]

Antarctica is a potentially rich source of natural resources. Platinum, copper, gold, iron ore, chromium and nickel, along with other minerals, have been discovered there. Hydrocarbons and coal appear only in small trace amounts. Most interesting, and perhaps ultimately most valuable, is that more than 70% of the world's fresh water supply is there. Of course, with all that valuable stuff about, as soon as it was possible to stay in Antarctica, countries began to claim territories there. Seven nations have made such claims, although the claims are not universally recognized as valid.[228] A legal framework was eventually constructed, entering into force in 1961, using a treaty – the Antarctic Treaty[229] – which neither recognizes nor disputes the territorial claims. The Treaty sets aside the continent as an area to be used only for peaceful purposes. Military activity is banned,[230] and freedom of scientific investigation and cooperation are required.

KEY LESSONS FROM REGULATION OF THE COMMONS

As noted *supra*, one must be careful in using analogies and metaphors for guidance. While they may inform and illuminate, no analogy or metaphor is a perfect fit. Surely there are ways in which the great commons are like cyberspace: each is a domain within which human activities transpire, for good or evil. Each relies upon and requires technology to enable the use and exploitation of the domain. Each offers benefits to those nations, organizations and individuals that can access them, and for each of the great natural commons, a regulatory framework has evolved that guides and controls human behavior within the commons. These likenesses offer the promise that analysis of their regulatory frameworks can guide and inform the development of a regulatory framework for cyberspace.

But we have also seen that there are significant differences among the commons and between each of the natural commons and cyberspace. The natural commons are all extensive in real space, while cyberspace (mostly) exists within a complex web of man-made wires, fiber optic cables, and electronic devices. Although these wires, cables and devices are each owned by someone and exist in real space with its developed legal jurisdictions, it is inherent in the design of the Internet that "location" in cyberspace is only loosely tied to real space in a detectable way, and so observed activities are difficult to attribute to specific individuals, organizations

227 http://www.state.gov/www/global/arms/treaties/arctic1.html.
228 https://www.cia.gov/library/publications/the-world-factbook/geos/ay.html.
229 http://www.state.gov/www/global/arms/treaties/arctic1.html.
230 Military personnel and equipment may be used for scientific research or any other peaceful purpose.

or nations. Distance in cyberspace seems unrelated to distance in real space, and the borders we so carefully defend in real space are effectively transparent in cyberspace. It follows inevitably that many of the schema and methodologies that serve us well in regulating the great natural commons are at least suspect, and may well be completely ineffectual, in cyberspace.

Nevertheless, we have seen that when nations perceive that it is in their common interest to develop internationally applicable regulatory frameworks, the means to do so exist. So, what might an effective international framework for regulation of behavior be like, given our experience with the frameworks guiding and regulating behavior in the great natural commons?

First, since every computer, system, server, wire and cable lies in or crosses existing jurisdictions in real space, the framework can and should, to the maximum extent possible, take advantage of those connections between cyberspace and real space. This follows the example of the laws of the sea and of the atmosphere, and implies that those portions of cyberspace that can be tied to nation-state jurisdictions will be subject to the laws of those jurisdictions, and that individuals and organizations who operate in cyberspace will be subject to the jurisdictions in which their operations take place. Making the laws of the various nations accessing, using and exploiting cyberspace coherent is a problem we will address in the next section of this paper. Even so, we recognize that even in real space some portions of the world are not subject to existing nation-state jurisdiction, and we must account for those portions of cyberspace that lie in international waters or in outer space, where international law applies, and develop appropriate rules for activities using those portions of cyberspace.

Second, we can develop a framework for regulating behavior in cyberspace that is as complex as it needs to be. As Albert Einstein famously said in another context, "Everything should be made as simple as possible, but no simpler."[231] The regulations for the law of the sea, for example, may be viewed as a transparency overlying real space: over land the laws of the relevant jurisdiction apply (except over Antarctica when jurisdiction is assigned by treaty), near to shore a slightly different set of rules apply, and beyond the near shore up to 200 miles from the coast still another set of rules applies, and then international law takes over for the high seas. Similarly, our framework need not consist only of hard-and-fast rules. In air traffic control, some communications relay binding instructions, while others are merely advisory. In cyberspace, we might want some hard requirements for implementation of policies, practices, procedures and technologies recognized to be effective in

231 http://rescomp.stanford.edu/~cheshire/EinsteinQuotes.html.

deterring, detecting and interdicting abuses and undesirable activities. In other cases, we may merely wish to inform users of steps and countermeasures they may wish to voluntarily take to enhance their own security and lessen their liability.

Third, we must recognize that the inherent nature of cyberspace and the media within which it exists limit our ability to regulate. As we saw in outer space, orbits necessarily cross borders and spaceflight would be impossible were concepts of sovereignty to permit nations to deny the users of space access to the portions of outer space above their territories like they can deny others the use of the atmosphere for airplane traffic above their territories. The routing of traffic through cyberspace is accomplished by algorithms largely beyond the control of those who access, use and exploit cyberspace. A framework in which Internet traffic could only pass through that portion of a nation's networks with the permission of that nation would render the Internet unusable.

The need for our framework to support free access and unhindered communications has especially interesting implications for cyberwar. All Internet communications must traverse various links and pass through various nodes as they travel from origin to destination. Since traffic is packetized, not all packets need pass through the same links or nodes. The user has little control over which links or nodes are used to complete the transmission. Civilian and military traffic share the same links and nodes, and military traffic – communications, espionage or information operations – may pass through links and nodes within the jurisdictions of belligerents, their allies, and neutral nations as well. The Internet protocols make no distinction among the users and their status with respect to cyberwar.[232] This makes cyberwar especially problematical with respect to the LOAC principle of distinction. The 1977 Additional Protocol I to the Geneva Convention[233] requires that parties to an armed conflict must distinguish between civilians and civilian property on the one hand, and combatants and military targets on the other, and that civilians and civilian property are forbidden targets. So called "dual-use" targets that serve both civilian and military purposes, now certainly including the Internet, may be attacked under certain circumstances:

> The answer depends on whether or not one applies Protocol I restrictions. If the [attacker is]is bound by Protocol I, a case can be made that such attacks are illegal, but the issue is very subject to interpretation. Let us consider the case of an attack upon an adversary's electrical system. Presuming that the justification of the attack is to destroy or degrade the adversary's military capability, then civilians are neither the "object of attack" nor is the primary purpose of the attack to "terrorize" them. Nevertheless, such an attack may violate Protocol I's provisions if it is indiscriminate

232 106 Mich. L. Rev. 1427, 1433.
233 http://www.icrc.org/ihl.nsf/COM/470-750073?OpenDocument.

> and/or if the incidental civilian effects are disproportionate to the concrete and direct military advantage of the attack. One can argue that such an attack is indiscriminate because it employs a method or means of combat (strategic attack of electrical generation facilities) the effects of which cannot be limited to the purely military objective. As a result, such an attack does not distinguish between military and civilian effects. Given this secondary, incidental effect upon civilians, one must apply the rule of proportionality, weighing the incidental effects on civilians with the concrete and direct military advantage the attack gives. Here there is divergence of view. [Cites Matthew C. Waxman, International Law and the Politics of Air Operations (Santa Monica, CA: Rand, 2000), 22.] The more restrictive view is that only direct civilian injuries, deaths, or destruction, namely those that occur immediately as a direct result of the attack (for example, from the explosion itself), should be considered. The second view is that all indirect civilian effects, namely those that occur over time as an indirect effect of the attack (for example, from loss of electricity) should also be considered. If one accepted the indirect view, then it might be very difficult to find a concrete and direct military advantage that outweighed the tens of thousands of civilian deaths that might be indirectly caused from loss of electricity. On the other hand, if one accepts only the direct view, such attacks would be very easy to justify provided one uses precision methods of attack. In sum, if one is bound by Protocol I, the legality of attacking dual-use targets is very much a matter of interpretation, as the disparity in views between the direct and indirect civilian effects creates a vast gray area in the law.
>
> If a state is bound by The Hague and Geneva Conventions but not Protocol I (like the US, for example), then the case against attack of dual-use targets is even weaker. Precision attack on an electrical facility doesn't rise to the level of "indiscriminate" or "wanton" destruction specified by The Hague and Geneva Conventions. Nor does it count as "willful killing" or "willfully causing great suffering or serious injury" to civilians because the harm to civilians is incidental to the military objective. Even if the incidental harm to civilians is significant, allowance for military necessity essentially neuters the civilian protections of the Conventions.[234]

So for an electrical facility, so for an Internet node.

As to the use of cyber versus kinetic weapons for the attack, international law does not turn on the nature of the weapon, but on the effect of the attack. If the attack takes place in cyberspace, should responses then be limited to cyber responses? After the Estonian incident, NATO took it as a rude awakening and started trying to figure out the implications of cyber incidents. They were thankful that Estonia did not exercise Article 5, but fully recognized that, had the Estonians done so, NATO would have been in a terrible position. If cyber incidents are sufficient to trigger Article 5, NATO could have ended up at war with Russia over the cyber attack on Estonia.

Following the Estonian and Georgian incidents, NATO has been working busily

234 http://www.airpower.au.af.mil/airchronicles/cc/Rizer.html

since trying to get new and improved doctrines in place so that future incidents are handled appropriately. They seem to be leaning toward a doctrine that asserts that cyber incidents are not "armed attacks" justifying kinetic responses and full application of the Laws of Armed Conflict. That position has interesting consequences. If a cyber incident is not an "attack" then, presumably, a cyber response isn't either. The LOAC applies in neither case. It's just kids on the playground; not WAR.

On the other hand, it seems that if a kinetic response is deemed appropriate after a cyber incident, then a cyber incident is, almost by definition, an "attack" triggering the LOAC. If the destruction caused by the incident is sufficiently widespread and destructive, it would be hard to argue that an attack had not occurred and that a kinetic response was not appropriate.

So, we are between the proverbial rock and hard place. If our ability to retaliate were sufficiently robust and the attacking state (or parties within a non-responsive attacking state) sufficiently unable to defend against our response, then we could just respond in kind (cyber only) – a kind of "mutually assured disruption" policy. But if either condition fails, a cyber incident could rapidly escalate into a full-scale shooting war, and that seems extreme. So the clear implication, it seems to us, is that we need to be sure a cyber incident can't lead to sufficiently widespread destruction as to justify a kinetic response. Defense precludes offense, so each nation must first have a strong focus on self-protection.

The nature of the Internet also makes more complex the notion of neutrality.[235] The Hague Conventions specify the rights and responsibilities of belligerent and neutral states with regard to neutrality. Under the Conventions, belligerents may not move troops, weapons, or other materials of war across neutral (land) territory,[236] and neutral states must enforce these rules.[237] Naval vessels may transit the waters of a neutral state provided they engage in no acts of hostility while in those waters.[238] But, with regard to telecommunications, Article 8 provides that," A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[239] Arguably, this principle extends to modern

235 The following discussion is based on Jeffrey T. G. Kelsey (2008) Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. 106 Mich. L. Rev. 1427.
236 1907 Hague Convention V, art. 2. http://avalon.law.yale.edu/20th_century/hague05.asp.
237 1907 Hague Convention V, art. 5. http://avalon.law.yale.edu/20th_century/hague05.asp.
238 1907 Hague Convention XIII, art. I and II. http://avalon.law.yale.edu/20th_century/hague13.asp.
239 http://avalon.law.yale.edu/20th_century/hague05.asp.

communications technologies, including the Internet.[240] But, to the extent that the information infrastructure of a neutral nation is used to move cyber weapons, or even information important to military operations like weather, imagery, or GPS navigation data, no exception applies and a neutral state that allowed a belligerent to move such information would open the neutral state to attack by the opposing belligerent parties to stop the flow.[241] To avoid the unintended consequences of the current LOAC framework, the, our new cyberspace framework may need take the position that what neutral parties need to do to maintain their neutrality merely is to avoid taking any action that would favor one belligerent or group of belligerents at the expense of others.[242]

Developing a regulatory framework for a great commons takes time, and significant efforts need to be expended at the national level in support of (and possibly prior to) efforts at the international level (the UNCLOS lesson). The development needs to follow real-life needs and balance the interests of multiple stake-holders (the ATC lesson). With careful attention to the inherent characteristics of cyberspace, and due care to recognize and avoid unintended consequences, it should be possible to create a regulatory framework that is realistic in application of rules that can actually work and which with due care can recognize and avoid unintended consequences.

LOOKING FORWARD

Creating a regulatory framework for cyberspace will only be possible if there is a shared recognition of the desirability – indeed, even the necessity – of doing so. Shared recognition of the necessity for international regulation of the use and exploitation of the seas and the natural resources within and under the seas led to international cooperation in developing a regulatory structure for the oceans, and eventually UNCLOS. Shared recognition of the need for coherent regulation of air traffic control led to the Chicago Convention. A mutual desire to keep nuclear weapons out of outer space led to the United Nations Treaties and Principles in Outer Space. And the shared recognition that Antarctica was best explored by scientists uninhibited by territorial aspirations or military utilization led to the Antarctic Treaty.

Several influential international organizations have promoted cyber security in

240 See Dept. of Defense Office of Gen. Counsel, An Assessment of International Legal Issues In Information Operations 11 (1999), http://www.maxwell.af.mil/ au/awc/awcgate/dod-io-legal/dod-io-legal.pdf at p. 10.
241 *Ibid.*
242 106 Mich. L. Rev. 1427, 1449.

their agenda. One of the most recent examples is the NATO 2020 report, whereby "NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."[243] Similar conclusions have been reached by the EU, UN, OECD and others. In addition to mutual recognition that a regulatory framework was desirable for balance of powers in the great natural commons, there has also been a shared sense that the frameworks need to protect the rights to access and use the commons by nations that are not great powers as well as those that are.

It is not at all clear that such a consensus exists today or is even possible with respect to cyberspace. It is clear that cyberspace can be used not just for commercial or recreational purposes, but for the exercise of national power through espionage, diplomacy, and even military exploitation. Nations with access to and deep understanding of information technology are better positioned to use and exploit cyberspace for national power than nations that have fewer such resources, and may be unwilling to give up their advantages before it is clear that the downside to such use outweighs their advantage. That clarity may be some time in arriving. But regulatory frameworks for the great natural commons did not arrive overnight either. It took fourteen years and the contributions of 150 nations to produce UNCLOS. Years of effort led to the Chicago Convention for air traffic control. It is clear, however, that such comprehensive frameworks cannot develop if countries are not interested in pursuing them.

Lacking a consensus that a comprehensive framework for regulation of behavior in cyberspace is desirable, humankind will continue to develop regulations for cyberspace in a piecemeal fashion. Already we have the Council of Europe's Convention on Cybercrime[244] addressing criminal activity in cyberspace. Thirty-four countries participated in the signing ceremony in November of 2001, but few countries have ratified the Convention, relying on it more as a guide to development of internal legislation than as a binding treaty. "Common criticisms are that the treaty fails to provide meaningful privacy and civil liberties protections, and that its scope is too broad and covers much more than computer-related crimes. The treaty also lacks a "dual criminality" provision, under which an activity must be considered a crime in both countries before one state could demand cooperation from another." [245]

243 http://www.nato.int/cps/en/natolive/official_texts_63654.htm#p1.
244 Council of Europe's Convention on Cybercrime http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
245 http://epic.org/privacy/intl/ccc.html.

Property in cyberspace is the subject of much controversy. The United Nations created the World Intellectual Property Organization (WIPO), established by the WIPO Convention[246] in 1967 to create a regulatory framework for protection of intellectual property. Currently, 184 nations participate in determining the strategic direction and activities of the Organization.

Regulation of commerce in cyberspace, often called e-Commerce, has been evolving for many years. Of course, commerce used and depended upon electronic communications beginning as early as the advent of telegraphic communications. With the growth of the Internet, commerce began to exploit cyberspace for exchange of purchasing, delivery and financial information, and the legal system had to adapt rules that had evolved over centuries as contract law to allow legally cognizable contracts made by parties using cyberspace communications.[247] United Nations Commission on International Trade Law (UNCITRAL) was established by the General Assembly in 1966 to harmonize the laws governing international commerce and reduce obstacles to the flow of trade.[248] The United Nations Convention on Contracts for the International Sale of Goods was created to provide "uniform rules which govern contracts for the international sale of goods and take into account the different social, economic and legal systems would contribute to the removal of legal barriers in international trade and promote the development of international trade."[249]

Currently missing and badly needed are clear rules for information operations related to national power, especially military operations in cyberspace. International Humanitarian Law which serves is so well in real space needs to be adapted to the unique characteristics of cyberspace. Special attention is needed to the issues of attribution and accountability, as well as the forensic policies, practices, procedures and technologies needed to make attribution and accountability work.

Such a piecemeal approach to regulation of behavior in cyberspace undoubtedly has undesirable outcomes. Regulations may be inconsistent, or even contradictory when developed in isolation. Serious gaps may leave certain areas unregulated. Were a consensus to arise that a common regulatory framework for cyberspace is desirable, we have excellent models provided by the great natural commons for creation of regulatory frameworks that could be used. While the differences that make cyberspace unique among the great commons make it impossible to import existing regulatory frameworks without modifications that take into account the

246 The WIPO Convention http://www.wipo.int/treaties/en/convention/trtdocs_wo029.html.
247 http://www.sagepub.com/upm-data/9598_019964Ch1.pdf.
248 http://www.uncitral.org/uncitral/en/about/origin.html.
249 http://www.cisg.law.pace.edu/cisg/text/treaty.html

unique nature of cyberspace, the process for creating regulatory frameworks is well-understood. Using the process could eventually lead to a coherent, comprehensive regulatory framework for cyberspace that facilitates its access and exploitation, ensuring that the benefits of cyberspace are available to all and that the risks of its use for criminal purposes or national power abuses are minimized.

CYBER SECURITY AND DEFENCE FROM THE PERSPECTIVE OF ARTICLES 4 AND 5 OF THE NATO[250] TREATY

Ulf Häußler[251]

INTRODUCTION

In the recently published report 'NATO 2020: Assured Security; Dynamic Engagement' which contains the analysis and recommendations of the group of experts on a new strategic concept for NATO[252], the experts observed that:

> "… the risk of a large-scale attack on NATO's command and control systems or energy grids could readily warrant consultations under Article 4 and could possibly lead to collective defence measures under Article 5."[253]

This observation points at the key challenges cyber activities pose from a legal perspective on international peace and security. It can easily be rephrased as a question: In what circumstances and under what conditions would NATO's collective security and defence mechanisms be triggered by cyber activities? The present paper will explore some initial answers to this question. For this purpose, it will revisit and explain the language of the North Atlantic Treaty in lights of relevant NATO practice, identify possible cyber threats and assess them against the thresholds contained in Articles 4 and 5 of the North Atlantic Treaty, and discuss key challenges which may arise in the course of developing NATO responses (noting that such challenges may also affect the effort to include the notion of effective deterrence[254] in the Alliance's approach to cyber defence). While based on legal analysis of the North Atlantic Treaty and relevant international law, this paper

250 The original title of the article "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the North Atlantic Treaty" was shortened by the editor for technical reasons.

251 Assistant Legal Advisor (Operational Law), Allied Command Transformation (NATO ACT, Norfolk/Va., USA). The views expressed herein are my own; they do not necessarily correspond with the official position of NATO or the Headquarters, Supreme Allied Commander Transformation. The author expresses his gratitude to Ms Simona Rocchi, Legal Advisor to NC3A, Mr Jude Klena, Counsel within the U.S. Navy, and Ms Katharina Ziolkowski, Legal Advisor within the German Armed Forces, for insightful comments and critique of an earlier version of this paper.

252 The experts report is available at http://www.nato.int/strategic-concept/expertsreport.pdf (last visited 16 June 2010).

253 Cf. the experts report at 45.

254 Cf. the experts report at 11 and 20.

focuses on the legal policy questions associated with the effort to fully integrate cyber defence in NATO's toolbox.

PRELIMINARY REMARKS

In coaching their above observation in the subjunctive mood, the experts have indicated that their analysis does not amount to a statement of NATO policy concerning the interpretation and application of Articles 4 and 5 of the North Atlantic Treaty. This being so, the observation indicates that to date no policy consensus of that nature exists in NATO[255]. In the absence of policy decisions and policy consensus, one important, probably the key contribution to the interpretation and application of international treaty law – aptly identified as represented by 'any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation' by Article 31(3)(b) of the Vienna Convention on the Law of Treaties – is missing.

In the context of international peace and security, the significance of policy decisions and policy consensus for the interpretation and application of international law oftentimes by and large overlaps with their nature as acts embodying the primacy of policy over the use of military force. While contemporary decisions to use a nation's and/or an alliance's capabilities in pursuance of collective defence may involve the interpretation and application of international law and as such also be expressions of legal policy, they equally reflect the insight, long ago shared by Carl v. Clausewitz, " ... that war is not merely an act of policy but *a true political instrument*, a continuation of political intercourse, carried on with other means".[256]

Considering the highly political nature of such decisions, the associated interpretation and application of Articles 4 and 5 of the North Atlantic Treaty may come with no less ambiguity than any equivalent effort made with respect to many another relevant law-making international treaty. To give but two examples for the prevailing level of ambiguity: neither has any "declared war"[257] occurred since 1949

255 Several scholars stress the importance of consensus regarding the interpretation and application of the rules concerning the jus ad bellum to the use of cyber capabilities. See e.g. Matthew Holsington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, in: 32 B.C. Int'l & Comp. L. Rev 439 (2009) at 439 and 454; William Yurczik & David Doss, Internet Attacks: A Policy Framework for Rules of Engagement (online at arxiv.org/pdf/cs/0109078; last visited 31 August 2010), at 17; cf. also Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, in: 106 Michigan Law Review 1427 (2008) at 1430 (noting the lack of consensus regarding the application of the *jus in bello* to cyber warfare).

256 Carl v. Clausewitz, On War, translated by Michael Howard and Peter Paret and published by Alfred A. Knopf in the Everyman's Library series, New York - London - Toronto 1993, Book One Chapter One Part 24 entitled "War is Merely the Continuation of Policy by Other Means" (my emphasis).

257 This language is borrowed from Article 2 of GCs I-IV.

(despite the considerable number of international armed conflicts in that time-frame) – if only because it may have been easier for States to obtain authorisation by the UN Security Council under Chapter VII or rely on their inherent right of self-defence (doing which also counters allegations that they might have breached Article 2(4) of the UN Charter) – nor has the UN Security Council made any significant use of the options available to it for the purpose of characterising a situation under Chapter VII of the UN Charter ("existence of any threat to the peace, breach of the peace, or act of aggression"[258]), options which it has by and large replaced by the phrase "threat to international peace and security"[259]. What is good for the UN Security Council would seem to be equally good for the North Atlantic Council: interpretation and application of pertinent legal bases will more likely be guided by practical policy concerns than by a desire to win an award for perfectionism in matters of legal doctrine. It follows that a search for circumstances and conditions in which cyber activities would trigger NATO's collective security and defence mechanisms will not necessarily yield an abundance of clear-cut criteria early on; rather the degree of clarity will grow as the related policy consensus matures.

ARTICLES 4 AND 5 OF THE NORTH ATLANTIC TREATY

The North Atlantic Treaty has established NATO as a collective security and defence alliance involving cooperation in matters of security and defence policies as well as military operations. Initially focused on defence of its nations' territories, NATO's role as a security provider has been transformed in recent years; it now includes the organisation's preparedness – where possible in a lawful and legitimate manner – to tackle, prevent, or pre-empt threats at their source[260].

NATO's collective security and defence mechanisms are primarily entrenched in Articles 4 and 5 of the North Atlantic Treaty[261]. Article 4 provides that:

> '[t]he Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened'.

Article 5 specifies that:

> '[t]he Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they

258 See Article 39 of the UN Charter.
259 The UN Security Council has used this language in multiple resolutions adopted in application of Chapter VII of the UN Charter.
260 Strategic Concepts 1993 and 1999.
261 For the full text of the North Atlantic Treaty see http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

> agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked …'.

These provisions indicate that it is the Nations' prerogative to determine whether they consider themselves exposed to a threat or under armed attack. However, they do not create any automaticism whatsoever concerning the response in such cases[262].

Whilst they are NATO's key legal bases, Articles 4 and 5 are not the sole legal bases for NATO action. As confirmed by consolidated practice, they are supplemented by Article 7 of the North Atlantic Treaty – which keeps the door open for NATO and NATO-led operations in support of the purposes of the United Nations – and appropriate implied powers of the organisation.

The emergence and growth of NATO's security policy *acquis* through policy decisions concerning strategy – embodied *inter alia* in the Strategic Concepts 1993 and 1999 as well as the Comprehensive Political Guidance 2006 – as well as operations – all NATO and NATO-led operations require approval by the North Atlantic Council – demonstrates the flexibility of the ensemble of these legal bases for decision-making on Alliance action[263]. NATO Nations' related decisions confirm that they wholeheartedly approve the flexible interpretation and application of the North Atlantic Treaty. The most important decisions of this nature are embodied in the integration of new members in the organisation by virtue of various Protocols to the North Atlantic Treaty to which all NATO Nations have become Parties. Although the Alliance's security policy *acquis* is not expressly mentioned in these Protocols, the process leading to their approval and adoption – the Membership Action

262 As stressed by Beckett, each NATO Nation is 'the judge of whether armed force is required or whether other action will suffice' (The North Atlantic Treaty, the Brussels Treaty, and the Charter of the United Nations, London: Stevens & Son, 1950, at 28) regarding the application of Article 5. See also Lawrence S. Kaplan, NATO 1948: The Birth of the Transatlantic Alliance (Rowman & Littlefield Publishers, Canham/MD 2007), at 204; and, by the same author, NATO Enlargement: The Article 5 Angle, in: The Atlantic Council of The United States, Bulletin Vol. XII, No. 2, February 2001, at 2-3. The entire Bulletin addresses the policy dynamics associated with the 'less than clear commitment by the United States' which nevertheless 'is still the symbol of U.S. commitment to its European partners' (at 3/4, respectively). The post-9/11 practice of NATO and its Nations has confirmed this position.

263 A detailed analysis of NATO's security policy *acquis* would exceed the objective and scope of this paper. Suffice it to say that this *acquis* entails not only the facilitation of coalition-style multinational support of collective self-defence (Operation Enduring Freedom) but also NATO/NATO-led operations which the North Atlantic Council may approve in support of collective self-defence (Operation Active Endeavour); a UN Security Council Resolution (e.g. IFOR/SFOR/NHQ Sarajevo; KFOR, ISAF; NTM-I; NTM-A; Operation Ocean Shield and its predecessors) or the principles of the United Nations (e.g. Operation Allied Force); a request made by a sovereign state (e.g. Operations Amber Fox/Fox/Allied Harmony; Pakistan Earthquake Relief) or an international organisation (e.g. the African Union). Such operations may cover the entire spectrum of education, training and exercises support; humanitarian relief; counter-insurgency; and other forms of low as well as high intensity conflict, in particular in the framework of Non-Article 5 Crisis Response Operations.

Plan which prepares potential new members to join NATO in accordance with a decision taken by all NATO Nations – requires implementation of NATO's security policy *acquis* by candidate countries[264]. NATO Nations' ratifications of the relevant Protocols should hence be considered as acts confirming the security policy *acquis* in its capacity as a necessary condition for joining NATO. Moreover, NATO Nations have on numerous occasions reinforced the Alliance's security policy *acquis* through their decisions to approve, and contribute forces to, NATO/NATO-led operations. In the absence of indications to the contrary, the policy decisions referred to should be regarded as suggesting the existence of subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions as envisaged by Article 31(3)(a) of the Vienna Convention on the Law of Treaties, and the associated conduct of NATO and its Nations should be regarded as supplementing practice of the nature contemplated by Article 31(3)(b) of the Vienna Convention on the Law of Treaties[265].

This paper argues that the North Atlantic Treaty's flexibility also empowers NATO – from both a policy and a legal perspective – to include the full spectrum of cyber security and defence policy as well as operations in its toolbox.

THREATS & THRESHOLDS

To date, few instances of practice in the application of the thresholds for NATO involvement and action, respectively, specified in Articles 4 and 5 of the North Atlantic Treaty, have been reported. As regards Article 5, NATO's response to the September 11 attack on the United States of America is the only known example. Article 4 has been formally used in one reported case; in February 2003, Turkey asked for consultations concerning its defence needs arising in light of the impending resumption of hostilities against Iraq[266]. The absence of further identifiable practice may be due to the fact that in engaging the North Atlantic Council regarding threats to their security NATO Nations seem not to have expressly invoked this provision: if only to keep the consultations they initiated focused on substance rather than the

264 Under the heading of 'Defence and military', the Membership Action Plan focuses on the ability of the country to contribute to collective defence and to the Alliance's new missions. This ability is contingent on the implementation of the Alliance's security policy *acquis*. See the online version of the NATO Handbook at http://www.nato.int/docu/handbook/2001/hb030103.htm (last visited 02 august 2010).

265 It would seem that Article 31(3) of the Vienna Convention on the Law of Treaties would not establish a very high threshold for the purposes of establishing that decisions or action represent subsequent agreement or practice, respectively, as indicated by the use of the word 'any' as qualifier in this respect.

266 See Paul Gallis, NATO's Decision-Making Procedure (CRS Report for Congress, Order Code RS21510, 05 May 2003; online at http://www.fas.org/man/crs/RS21510.pdf (last visited 29 August 2010)), at 1.

question of whether the Article 4 threshold was actually crossed. For instance, in discussions the fact that the North Atlantic Council discussed the 2007 cyber attack faced by Estonia has repeatedly been cited as an example of Article 4 consultations despite the fact that neither Estonia nor the Council as a whole mentioned this provision. As a result, there is rather limited NATO practice to rely on as the primary source of interpretation concerning Articles 4 and 5 of the North Atlantic Treaty.

NATO AND UN LEGAL BASES COMPARED

In the near complete absence of practice, it is apt to explore further sources of interpretation. Apart from utilising scholarly writing which sheds light on the drafting history of the North Atlantic Treaty, comparative analysis of the development of related UN Charter provisions might be a source of inspiration for the interpretation of these provisions.

Articles 4 and 5 of the North Atlantic Treaty have a significant terminological overlap with Articles 2(4) and 51 of the UN Charter, respectively. Since such terminological overlap indicates that there may be a conceptual overlap, as well, the interpretation and application and are to a large extent capable of developing in unison. Whether, and to what extent, they have indeed developed along the same lines is revealed by policy decisions interpreting and applying them to individual situations. The UN and NATO responses to the attack on the United States on 11 September 2001 provide an ample example of a partly unison, partly different development of both treaties. As will be demonstrated shortly, both the UN Security Council and the North Atlantic Council have taken decisions bringing these attacks within the ambit of the notion of armed attack under Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty. However, neither of these decisions contains an express determination of why the threshold of armed attack was crossed. Accordingly, it is a matter of analysis whether they can be considered to address such legal questions arising with regard to responsibility and attribution as are associated with the fact that the attack was carried out by operatives of a non-governmental party (Al Qaeda), an organisation enjoying material support of the *de facto* government of Afghanistan at the time (the Taliban). Similar questions may arise with respect to cyber security and defence in light of the both empirical and practical relevance of the conduct of non-governmental actors in this field.

DRAFTING HISTORY

The drafting history of the North Atlantic Treaty reveals that threshold questions may not have been the predominant concern in developing the language of

Articles 4 and 5. The most important sources appear to be W. Eric Beckett's analysis concerning the question of whether NATO is a 'regional organization' as defined in Chapter VIII of the UN Charter (a question which he answers in the negative)[267], and Lawrence S. Kaplan's analysis of the level of commitment digestible in the U.S. Senate at the time of the negotiations[268].

Beckett, at the time a legal advisor to the Ministry of Foreign Affairs of the United Kingdom of Great Britain and Northern Ireland, observes that Article 4 has much in common with certain provisions of other collective security agreements[269]; he does not, however, address possible overlaps of Article 4 (or any of the other provisions discussed) and provisions on the UN Charter. At the same time, Beckett explores what relationship may exist between the consultation mechanism established by Article 4 and the right to engage the United Nations in case of looming security threats under Article 35 of the UN Charter[270]. The latter, in his view, does not 'in any way preclude any group of States from consulting on a potential threat to anyone of them' such as e.g. in accordance with Article 4 of the North Atlantic Treaty. According to Beckett: '[s]uch a consultation may have, amongst other things, a bearing on the question whether or not the threat should be brought before the Security Council', and '[n]o doubt if the consultation leads to the conclusion that the threat is sufficiently serious, one or other or all of the parties will exercise the right which they have under the Charter to bring the matter before the Security Council'.[271]

The analysis of Article 5, which 'is the collective self-defence obligation in case of armed attack'[272], likewise reveals similarities. Beckett rightly observes that 'Article 5 of the Treaty uses the same words "armed attack" as occur in Article 51 of the Charter and expressly purports to be based on that Article'[273]. This is confirmed by

267 See in particular Beckett, at 34.
268 Lawrence S. Kaplan, NATO Enlargement: The Article 5 Angle, in: The Atlantic Council of The United States, Bulletin Vol. XII, No. 2, February 2001, *passim*. See also, by the same author, NATO 1948: The Birth of the Transatlantic Alliance (Rowman & Littlefield Publishers, Canham/MD 2007).
269 According to Beckett, Article 4 'is rather similar to the second paragraph of Article 7 of the Brussels Treaty and has certain analogies with Article 6 of the Rio Treaty' (at 26sq). As regards Article 6 of the Rio Treaty (Inter-American Treaty of Reciprocal Assistance, signed at Rio de Janeiro, 02 September 1947; reproduced in Beckett, ibidem, at 51sqq), the difference in wording between Article 4 of the North Atlantic Treaty and Article 6 of the Rio Treaty is not tantamount to any real differences of substance and meaning (*ibidem*, at 21). At any event, as far as possible to establish there is no officially published practice under Article 6 of the Rio Treaty which could be relied on in support of the interpretation of Article 4 of the North Atlantic Treaty.
270 Article 35 of the UN Charter provides that UN member states may bring any dispute, or any situation which might lead to international friction or give rise to a dispute, to the attention of the Security Council or of the General Assembly.
271 Beckett, at 27.
272 Beckett, *ibidem*.
273 Beckett, at 29. See – in a different context (collective self-defence in support of NATO Nations which at the time were not members of the United Nations Organization) – *ibidem* at 31.

Kaplan's observation that the U.S. Senate was determined to ensure that Article 5 would be fully compatible with Article 51 of the UN Charter[274]. Successfully so, as demonstrated by Beckett's analysis of the statement in Article 5 that 'an armed attack against one or more of the Parties shall be considered to be an attack against them all': this language expresses 'precisely what the *inherent* right of *collective* self-defence means'[275].

When they embarked on turning the right of collective self-defence into the foundation of a collective self-defence obligation, NATO Nations have invited questions regarding the nature of this obligation. Kaplan, who compares Article 5 to the collective defence provisions of the Rio Pact and the Brussels Treaty, explains why it was easier for the U.S. to accept a moral rather than a legal obligation, viz. in light of the delicate balance between the constitutional powers of the U.S. Congress concerning declarations of war and the mechanism for setting collective self-defence in motion[276]. By contrast, Beckett's analysis, according to which the obligation under Article 5 is 'several and not merely joint'[277], indicates by using these legal categories that he considers collective defence within NATO to be a legal obligation. Whilst the true nature of the obligation under Article 5 of the North Atlantic Treaty was never determined, it may not have much practical bearing in the first place. NATO Nations have always considered it to be their sovereign decision what support they would provide in an actual case of collective self-defence, and in the one and only practical case, they have not hesitated to provide support in an apparently satisfactory manner.

As indicated earlier, Beckett's and Kaplan's observations and analysis focus on questions not involving the actual meaning of the substantive thresholds contained in Articles 4 and 5 of the North Atlantic Treaty. As regards Article 4, Beckett focuses on the consultation process envisaged by this provision rather than the threshold which may justify that a NATO Nation engages this process by way of requesting consultation. Beckett's analysis of Article 5 confirms that this provision establishes the same threshold as, and has further similarities with, Article 51 of the UN Charter; however, his observations concerning the notion of 'armed attack' in a footnote which merely repeats the essence of the discussion in the U.S. Senate's Foreign

274 Lawrence S. Kaplan, NATO 1948: The Birth of the Transatlantic Alliance (Rowman & Littlefield Publishers, Canham/MD 2007), at 217.
275 Beckett, *ibidem* (emphasis in the original). Moreover, as confirmed by Beckett, the similarity between Article 5 of the North Atlantic Treaty and Article 51 of the UN Charter also extends to the reporting requirement concerning measures taken in collective self-defence and the provision that such measures shall be terminated when the Security Council takes enforcement action (*ibidem*).
276 Lawrence S. Kaplan, NATO Enlargement: The Article 5 Angle, in: The Atlantic Council of The United States, Bulletin Vol. XII, No. 2, February 2001, at 3.
277 Beckett, at 28.

Relations Committee[278] indicate that this threshold did not pose major interpretive challenges at the time of drafting.

COLLECTIVE SELF-DEFENCE IN NATO PRACTICE

The attack on the United States of America on 11 September 2001 (hereinafter referred to as '9/11') represents the only case in which NATO's collective self-defence mechanism was used. The response to 9/11 demonstrates how the UN Security Council and the North Atlantic Council as well as multiple Nations have interpreted the notion of 'armed attack', key to the application of Article 51 of the UN Charter and Article 5 of the North Atlantic Treaty, respectively, in the same adaptive way so as to capture the genuine characteristic elements of the attack.

Following the 9/11 attack, the UN Security Council adopted UNSCR 1368 (2001) dated 12 September 2001 in which it recognised 'the inherent right of individual or collective self-defence in accordance with the Charter' and determined that it '*regards* such acts, like any act of international terrorism, as a threat to international peace and security'[279]. This resolution differentiates between the Chapter VII and self-defence thresholds; while it determined the former to have been crossed[280], it did not make an express determination concerning the latter. On the same day as the UN Security Council, the North Atlantic Council 'agreed that if it is determined that this attack was directed from abroad against the United States, it shall be regarded as an action covered by Article 5 of the Washington Treaty'[281], which it indeed determined, following a briefing on the results of investigations into the attack, on 02 October 2001[282]. Subsequently, the North Atlantic Council authorised Operation Active Endeavour, a maritime interdiction operation in the Mediterranean. NATO also informed the UN Security Council of its invocation of Article 5 of the North Atlantic Treaty[283]. The North Atlantic Council's decision also provides the umbrella for NATO Nations' support to Operation Enduring Freedom,

278 Beckett, at 28 (footnote 12).
279 See para 1 (emphasis in the original) and the last preambular paragraph of UNSCR 1368 (2001), respectively.
280 The UN Security Council has subsequently confirmed this determination. See UNSCR 1373 (2001).
281 See NATO Press Release (2001)124 dated 12 September 2001, online at http://www.nato.int/docu/pr/2001/p01-124e.htm (last visited 07 July 2010).
282 See NATO Topic: Collective Defence, online at http://www.nato.int/cps/en/SID-85648058-8934EDC9/natolive/topics_59378.htm (last visited 07 July 2010).
283 In the Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005), Canada has made reference to 'the notification by the Secretary-General of the North Atlantic Treaty Organization (NATO) to the Secretary-General of the United Nations on the invocation by NATO of article 5 of the North Atlantic Treaty' (*ibidem*). The notification was not circulated in the UN Security Council and, according to information generously provided by the UN Regional Information Centre Brussels to the author, is not accessible in the UN Archives Database, either.

the United States self-defence effort against the *de facto* government of Afghanistan (the Taliban) – the State responsible for the attack – and Al Qaeda – the terrorist organisation whose operatives had perpetrated the attack[284]. Canada's Article 51 report to the UN Security Council is particularly point-on since it expressly links the use of Article 51 to the North Atlantic Council's decision concerning Article 5[285]. Multiple Nations reported to the Security Council that they had taken measures in accordance with Article 51 of the UN Charter[286]; As a result, NATO's collective defence mechanism covers both NATO/NATO-led operations in support of a NATO Nation's self-defence[287] and a NATO umbrella for NATO Nations' support of another NATO Nation's self-defence.

284 The information concerning the responsibility of the Taliban and Al Qaeda available at the time to both the North Atlantic Council and the UN Security Council is reproduced in the Annex to the Letter dated 8 October from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (UN document S/2001/949). On attribution to the State of Afghanistan through its *de facto* government see my paper Der Schutz der Rechtsidee, in: Zeitschrift für Rechtspolitik (ZRP) 2001, 537-541.

285 See the Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005).

286 Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council (UN document S/2001/946); Letter dated 7 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (UN document S/2001/947); Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005); Letter dated 23 November 2001 from the Permanent Representative of France to the United Nations addressed to the President of the Security Council (UN document S/2001/1103); Letter dated 23 November 2001 from the Permanent Representative of Australia to the United Nations addressed to the President of the Security Council (UN document S/2001/1103); Letter dated 29 November 2001 from the Permanent Representative of Germany to the United Nations addressed to the President of the Security Council (UN document S/2001/1103). See also the Letter dated 17 October 2001 from the Permanent Representative of Slovenia to the United Nations addressed to the President of the Security Council (UN document S/2001/987).
Whilst it would exceed the scope and purpose of this paper to provide a full analysis of the legal nature of Operation Enduring Freedom as well the non-U.S. contributions thereto, it may suffice to note that many Nations which later adopted the position that the armed conflict between the U.S. and Afghanistan had come to an end when the *de facto* government was replaced by the Interim Authority established by the Bonn Agreement dated 05 December 2001 continued to contribute forces to Operation Enduring Freedom in the Afghan theater where fighting continued against forces which had been aligned with the ousted *de facto* government and/or were composed of, or comprised, Al Qaeda operatives. Since actions speak louder than words, the Nations in question have acknowledged – regardless of any public statements their governments may have made later – by way of continuing to contribute these forces with a mandate to support U.S. self-defence, the nature of the armed conflict in Afghanistan as a non-international armed conflict in exercise of the right of self-defence against a non-governmental actor.

287 For a similar assessment see the 'Fourth report on responsibility of international organizations' (UN document A/CN.4/564) submitted to the International Law Commission by Giorgio Gaja, Special Rapporteur, at para 19.

COLLECTIVE SECURITY IN NATO PRACTICE

Collective security within NATO is primarily captured by Articles 4 and 7 of the North Atlantic Treaty. Article 4 establishes the mechanism for consultations concerning threats to the territorial integrity, political independence or security of any NATO Nation. Article 7 specifies that the North Atlantic Treaty:

> 'does not affect, and shall not be interpreted as affecting in any way the rights and obligations under the Charter of the Parties which are members of the United Nations, or the primary responsibility of the Security Council for the maintenance of international peace and security'.

This clause enables NATO Nations to utilise the Alliance in fulfilling any obligations they may have under the UN Charter. – The legal bases just discussed are supplemented by implied powers associated with the North Atlantic Treaty which enable the Alliance to take appropriate action in support of its purposes, in particular collective security and defence of its members.

As will discusses shortly, Article 7 of the North Atlantic Treaty provides an appropriate plug-in point for NATO Nations to leverage the Alliance in fulfilling their obligations under the UN Charter. In particular, this provision confirms that NATO's implied power to launch operations designed to enhance collective security may also be used when such operations coincidentally also support the purposes of the United Nations[288].

The Article 4 mechanism for collective security through consultations does not pose major legal challenges. In the single reported case, the consultations requested by Turkey were conducted in NATO's Defence Planning Committee which on 16 February 2003 requested military advice from NATO's Military Authorities[289] and on 19 February 2003 authorised the implementation of defensive measures[290], namely the deployment of AWACS, Patriot missiles, and other defensive systems[291]. However, it appears that an earlier request to provide NATO support to Turkey met

288 In the practice of the North Atlantic Council, the assessment that NATO and UN purposes converge is usually expressed by way of a reference to the relevant resolution of the UN Security Council. See, for example, the fact sheet concerning the NATO Training Mission in Iraq at http://www.nato.int/cps/en/natolive/topics_51978.htm (last visited 31 August 2010).

289 See the DPC Decision Sheet at http://www.nato.int/docu/pr/2003/p030216e.htm (last visited 29 August 2010).

290 See Press Release (2003)013 at http://www.nato.int/docu/pr/2003/p03-013e.htm (last visited 29 August 2010).

291 See Paul Gallis, NATO's Decision-Making Procedure (CRS Report for Congress, Order Code RS21510, 05 May 2003; online at http://www.fas.org/man/crs/RS21510.pdf (last visited 29 August 2010)), at 2.

resistance – which, however, was not based on legal arguments[292].

On comparison with the thresholds contained in the UN Charter, threats to the territorial integrity, political independence or security certainly comprise any threat or use of force against the territorial integrity or political independence prohibited by Article 2(4) of the UN Charter, and likewise any threat to the peace, breach of the peace, or act of aggression as contemplated by Article 39 of the UN Charter – in both cases specifically when they do not amount to an armed attack[293] on a NATO Nation. Moreover, as indicated by Beckett's discussion of a possible conflict between the Article 4 mechanism and the right to engage the United Nations in case of looming security threats, each NATO Nation may also seek consultations if it finds itself in a 'dispute, the continuance of which is likely to endanger the maintenance of international peace and security' (cf. Article 33 of the UN Charter), provided it is of the opinion that such dispute involves at least an emerging threat to its territorial integrity, political independence or security.

The mechanism for collective security through utilising NATO in fulfilling obligations under the UN Charter is rooted in the link between Article 7 of the North Atlantic Treaty and Article 48 of the UN Charter. Article 48 specifies that 'decisions of the Security Council for the maintenance of international peace and security' (paragraph 1) 'shall be carried out by the Members of the United Nations directly and through their action in the appropriate international agencies of which they are members' (paragraph 2). Whilst the term 'international agency' seems dated from a contemporary perspective, it should be beyond doubt that it is not only capable of covering international organisations such as NATO but also has been

292 As reported, it could have been misunderstood as 'the equivalent of acknowledging that Iraq had impeded U.N. weapons inspections' – which was not proven according to the objecting governments – and might have amounted to a pretext for the impending resumption of hostilities against Iraq. Paul Gallis, NATO's Decision-Making Procedure (CRS Report for Congress, Order Code RS21510, 05 May 2003; online at http://www.fas.org/man/crs/RS21510.pdf (last visited 29 August 2010)), at 1.

293 For the differentiation between the thresholds defined in Articles 2(4) and 51 of the UN Charter, respectively, see the judgment of the International Court of Justice in the '*Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*' – ICJ Rep. 1986, 14-150, at para 210.

applied by the UN Security Council on the basis of this interpretation[294]. It follows that the observation that Article 48 of the UN Charter may contain 'an anticipatory reference to the regional agencies which come under Chapter VIII'[295] should not be misread such as to imply that its scope have to be considered limited thereto[296]. Conversely, Article 7 of the North Atlantic Treaty and Article 48(2) of the UN Charter build a bridge connecting the substantial legal bases for non-self defence action in the said international agreements. The North Atlantic Council has repeatedly used the powers implied in the North Atlantic Treaty to take action enhancing NATO's and its Nations' security, including by way of operations involving the use of force, namely in the form of Non-Article 5 Crisis Response Operations.

As a result, NATO's collective security mechanisms comprise consultations under Article 4 and utilising the organisation's implied powers *inter alia* to coincidentally fulfil its Nations' obligations under the UN Charter. Once again, the interpretation and application of the relevant provisions of the North Atlantic Treaty and the UN Charter, respectively, are in harmony; and the practice in the UN Security Council, the North Atlantic Council, and among the NATO Nations (as well as the States which have contributed forces to NATO-led operations) is sufficiently well entrenched to supplement these relevant provisions.

CONCLUSION AD INTERIM: NATO'S SECURITY POLICY ACQUIS

As indicated by the discussion of the practice regarding NATO's collective security

294 By way of example, the UN Security Council has implicitly referred to NATO as the designated lead organization of the Implementation Force (IFOR) for the Dayton Peace Agreement in Bosnia and Herzegovina in welcoming 'the willingness of the Member States acting through or in cooperation with the organization referred to in Annex 1-A of the Peace Agreement' (see para 12 of UNSCR 1031). The words 'acting through' in this paragraph clearly resemble the phrase 'through their action' in Article 48(2) and should, given the absence of any indications to the contrary, hence be regarded as an indication that the UN Security Council had Article 48 in mind in adopting resolution 1031. – Later resolutions contained express authorisations of NATO *sub specie* 'relevant international organizations' (para 7 of UNSCR 1244 – Kosovo Force (KFOR)) or acknowledged NATO's role as the lead organisation by way of noting relevant correspondence (cf. the eighth and ninth preambular paragraphs of UNSCR 1510 (International Security Assistance Force (ISAF)) concerning the letter dated 10 October 2003 from the Minister for Foreign Affairs of Afghanistan – UN document S/2003/986, annex – which contains the statement that '[t]he Afghan authorities have repeatedly welcomed the assumption of strategic command, control and coordination of ISAF by the North Atlantic Treaty Organization (NATO)' – and the letter dated 06 October 2003 from the NATO Secretary General regarding the expansion of ISAF's mission – UN document S/2003/970).

295 Beckett, at 12.

296 Apart from being counterintuitive, such a limitation of the scope of Article 48 of the UN Charter has no foundation in its language. Speaking of 'appropriate agencies', it does not anticipate the formula used in Article 52 of the UN Charter, namely 'regional arrangements or agencies'. As a result, the criteria under Chapter VIII of the UN Charter are without prejudice to the question of whether 'agencies' – or, in more modern language, international organisations – are 'appropriate' for the purposes of taking '[t]he action required to carry out the decisions of the Security Council for the maintenance of international peace and security'.

and defence mechanisms, NATO has progressively developed a well-balanced security policy *acquis* which adapts the said mechanisms so as to maintain coverage of the whole spectrum of threats the Alliance and its Nations may be exposed to. It does not require much creative thinking to argue that the decisions and practice contributing to this security policy *acquis* 'shall be taken into account' (Article 31(3) of the Vienna Convention on the Law of Treaties) in confirming the appropriate interpretation of the relevant legal bases.

As an integral part of this security policy *acquis*, NATO's repertoire of responses comprises – in addition to any diplomatic means of the Alliance's choice – both the facilitation and/or support of action taken by its Nations individually or in concert, and NATO/NATO-led operations. The latter may coincidentally support the collective security of NATO and its Nations as well as the principles of the United Nations, including as applied to an individual situation by the UN Security Council in a Chapter VII resolution.

The emergence and consolidation of this security policy *acquis* demonstrate the flexibility of the North Atlantic Treaty. Moreover, taking into account the Vienna Convention on the Law of Treaties, they should also be considered to reflect the emergence and consolidation of a legal policy consensus regarding the interpretation and application of the North Atlantic Treaty.

INTEGRATING CYBER SECURITY AND DEFENCE IN NATO'S SECURITY POLICY ACQUIS

Forging a policy consensus concerning the interpretation and application of NATO's legal bases to cyber activities may require taking into account multiple thresholds, including such pertaining to other domains than international law. As discussed earlier, NATO yet has to include collective cyber security and defence in its policy consensus regarding the interpretation and application of its legal bases. To do so, NATO may have to address a range of challenges associated with international law, legal and political policy, and institutional arrangements. Whilst no official communiqué tackles the whole range of these challenges, different aspects thereof are addressed in the experts report and national level policy statements or documents. To date, according to the experts "cyber attacks against NATO systems occur … most often below the threshold of political concern"[297]. This cautious language identifies 'NATO systems' rather than NATO as affected by cyber attacks; it does not discuss NATO Nations and/or their computer and

297 See the experts report, at 45.

communications systems. It is hence without prejudice to assessments made at national level. Indeed, from one or more perspectives the threshold of political concern may well have been crossed more than once. For instance, His Excellency Mr. Toomas Hendrik Ilves, President of the Republic of Estonia, has observed that there have already been cases of actual or prevented aggression against nation-states carried out in cyberspace: "Were they to have been carried out with kinetic weapons, we in NATO would be faced minimally with an Article 4 and most likely with an Article 5 scenario."[298] By contrast, the Federal Government of the Federal Republic of Germany has recently addressed cyber attacks directed from abroad in the 2010 edition of the 'Verfassungsschutzbericht' (covering the year 2009)[299], a report commissioned by the Federal Ministry of the Interior on the basis of police and intelligence reporting which tackles threats to Germany's constitutional order – i.e. significant threats to internal, or homeland, security.

POLITICAL POLICY AND INSTITUTIONAL ARRANGEMENTS

The fact that a given cyber threat or incident crosses the threshold of political concern is without prejudice to its political and legal characterisation for the purpose of developing an appropriate response. Much will depend on political policy perceptions – are cyber threats and incidents predominantly perceived as human rights (i.e. data privacy) issues, matters of law enforcement and/or homeland security[300], or matter of national security and defence – and the different roles played by the government agencies involved on the examination and assessment of cyber threats and incidents, and competent to adopt or contribute to actual responses. Accordingly, it may be for multiple reasons that NATO faces challenges in developing consensus regarding the full integration of cyber security and defence in its respective mechanisms, as well as the necessary institutional arrangements.

First, in an environment where any security and defence discourse is to a great extent predetermined by the level of political concern, there may simply have been a limited number of opportunities to actually put cyber security and defence prominently on NATO's agenda. Second, quite similar to threats arising from international terrorism, threats arising in and out of the cyber space may give rise

298 See http://www.ccdcoe.org/conference2010/329.html; cf. http://www.nato.int/cps/en/SID-B2AD4DE6-E0B91B4E/natolive/news_64615.htm? (last visited 30 August 2010)

299 Verfassungsschutzbericht 2009 (preliminary version), at 307sq; available at http://www.bmi.bund.de/cae/servlet/contentblob/1098014/publicationFile/91389/vsb2009.pdf (last visited 31 August 2010).

300 JP 1-02 defines homeland security as: 'A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur.' Reference is also made to JP 3-28 (*ibidem*).

to both internal, or homeland, and external security concerns, and thus trigger the oftentimes complex delineations of competence between the defence, law enforcement, and intelligence sectors which many NATO Nations have developed into strong checks and balances amounting to a separation of powers *en miniature* within their executive branches of government. Whilst obviously such domestic arrangements lack the capacity to affect the interpretation and application of the North Atlantic Treaty[301], they may nevertheless *de facto* challenge NATO Nations' Defence Ministries' as well as Armed Forces' ability to put cyber security and defence on NATO's policy, concept, and doctrine agendas. To date, no well-entrenched method, structure or process for overcoming this *de facto* challenge – e.g. through involvement of foreign intelligence, homeland security and/or law enforcement stakeholders – exists within NATO. Third, there is a near complete lack of NATO-wide, standardised doctrine for cyber warfare. The resulting absence, amongst NATO Nations, of a militarily agreed and legally cleared (Article 36 of GP I) understanding concerning the means and methods of cyber warfare may also contribute to the lack of political policy consensus. The appetite for engaging in hostilities which might be perceived as potentially involving legally doubtful means and methods of warfare may be limited. Ultimately, the absence of consensus regarding *jus in bello* may thus have repercussions on the likelihood that consensus can be reached concerning *jus ad bellum* as well as collective security and defence.

INTERNATIONAL LAW AND LEGAL POLICY

New technology has met laws of greater age on various occasions. Sometimes its impact was smooth, at other times the integration of new technology in existing legal frameworks failed in light of the absence of appropriate plug-in sockets. These alternatives were also discussed with respect to cyber technology. Ever since the arrival of cyber technology in the armouries the effects of their use has been compared to the effects of kinetic warfare. Over the years, the analysis of cyber warfare revealed that, whilst technically speaking, cyber activities have a direct effect on electrons only, the indirect effects caused by them may entail death or injury as well as damage or destruction. Moreover, the use of cyber technology may impact a nation's governability, i.e. deny its government's effectiveness and push it onto the slippery slope towards destabilisation and failure.

301 See Article 27 of the Vienna Convention on the Law of Treaties.

Following an earlier period of significant discussions of *jus ad bellum*[302] (and *jus in bello*[303]) concerning cyber attacks around the turn of the millennium, the 2007 cyber attack faced by Estonia as well as the use of cyber capabilities in the context of the armed conflict between Russia and Georgia in 2008 have led to renewed interest in matters of cyber warfare. This section will discuss four types of scenarios involving the use of cyber technology from a *jus ad bellum* perspective. It will analyse these scenarios, which are based on an abstraction from examples rather than generic, with a view to establishing whether, as well as in what circumstances and under what conditions, certain usages of cyber technology may be eligible as elements of a (legal) policy consensus regarding NATO's collective security and defence mechanisms.

The first type of scenarios covers the use of cyber technology as an enabler for traditional kinetic force used to launch a campaign. One operation of that nature may have occurred when Israel struck a construction site at Tall al-Abyad, Syria, on 06 September 2007. It appears that the attacking aircraft got through Syria's air defence radars without being detected. According to a report in Aviation Week, an information and service providing business[304], this may have been due to an airborne network attack system which 'allows users to invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen .... The process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading messages algorithms that allow a number of activities including control.'[305] Just like this real world situation, the as of yet theoretical example of a cyber attack disabling

302 The key reference is Michael N. Schmitt, Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Columbia Journal of Transnational Law 885-937 (1999). See also Dimitrios Delibasis, State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century (available at www.peacestudiesjournal.org.uk/dl/Feb%2006%20DELIBASIS.pdf – last visited 31 August 2010).

303 See, for instance, Michael N. Schmitt, Wired Warfare: Computer network attack and *jus in bello*, in: 84 International Review of the Red Cross 365-399 (2002); Steven M. Barney, Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace?, 48 Naval Law Review 43-87 (2001); William Yurcik & David Doss, Internet Attacks: A Policy Framework for Rules of Engagement (available at arxiv.org/pdf/cs/0109078 – last visited 31 August 2010).

304 See http://www.aviationweek.com/aw/About_Us_Home.do (last visited 29 August 2010).

305 See the report 'Why Syria's Air Defenses Failed to Detect Israelis' by David A. Fulghum, posted 03 October 2007; available at http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a2710d024-5eda-416c-b117-ae6d649146cd&plckScript=blogScript&plckElementId=blogDest. This report is quoted at http://www.theregister.co.uk/2007/10/04/radar_hack_raid/ and http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/; a detailed report is available at http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw112607p2.xml&headline=Israel%20Shows%20Electronic%20Prowess&channel=defense (all visited 29 August 2010)

the key platform in a ballistic missile launch reporting network[306] would be of a similar nature.

Whilst 'locating enemy emitters' and copying 'what enemy sensors see' are acts of cyber espionage and in that capacity below the threshold of use of force, once the intruders 'take over as systems administrator' – including through 'direct[ed] data streams' – the assessment may change. Any such act of cyber espionage faced by a NATO Nation may, depending on (information and intelligence regarding) the circumstances as well as the relevant strategy and doctrine, amount to a threat of the nature contemplated in Article 4 of the North Atlantic Treaty rather than a mere nuisance. By contrast, seizing control through the use of cyber technology may in itself amount to an illegal use of force and at the same time create a situation where the 'necessity of self-defense [is] instant, overwhelming, leaving no choice of means, and no moment of deliberation'[307]. Exercising control once it has been seized, including by way of manipulating sensors or including false targets, may – again depending on the circumstances as well as the relevant strategy and doctrine – either indicate that an armed attack is imminent, or be an integral part of an actual armed attack.

The second type of scenarios covers hybrid threats of which the use of cyber technology may be one contributing factor. According to a recent conceptual document submitted by NATO's two Supreme Headquarters to the Military Committee, "Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[308] This conceptual approach confirms that 'hybrid threats arise from a blend of simultaneous actions'[309]. The notion of 'blend of simultaneous actions' reflects that in the context of a hybrid threat, weakening NATO and its Nations may be a means to achieve a range of different ends rather than one single strategic objective from the perspective of the adversaries involved. Accordingly, just as adversarial activities contributing to a hybrid threat does not necessarily indicate the existence of any kind of alliance among the adversaries in question, the use of cyber technology as part of such blend does not represent a cyber

306 See the discussion by Thomas C. Wingfield, Legal Aspects of Offensive Information Operations in Space, at 11 (available at www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.doc – last visited 31 August 2010).

307 See Secretary of State Daniel Webster's 'Letter to Henry Stephen Fox', in K.E Shewmaker (ed.). The Papers of Daniel Webster: Diplomatic Papers, vol. 1. 1841-1843 (1983), at 62.

308 BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats (Enclosure 1 to document no. 1500/CPPCAM/FCR/10-270038 – 5000 FXX 0100/TT-6051/Ser: NU0040 dated 25 August 2010 – marked 'NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC'), at para 7.

309 BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats, at para 19.

line of operations. That said, the use of cyber technology in this context would nevertheless either be a multiplier or its effects would be multiplied by any other contributing factor(s). Ultimately, the assessment would depend on the mutually reinforcing effects of the variety of factors capable of contributing to a hybrid threat whose materialisation may amount to an adversary's first strike. Article 5 of the North Atlantic Treaty may be triggered in this context if the scale and gravity of the overall effect of that first strike corresponds with the kinetic equivalent.

The third type of scenarios covers the use of cyber capabilities to degrade or deny decision-making and associated command and control capability, and/or achieve information superiority in the field of strategic communications, both of which may make a significant contribution to campaign success. One operation of that nature may have occurred when armed conflict broke out in Georgia in August 2008. Even prior to the hostilities, a 'short occasion of turbulence' occurred on 19 July 2008[310]. According to unnamed experts, the cyber attacks conducted during the period of hostilities[311] may 'have reduced Georgian decision-making capability, as well as its ability to communicate with allies, thereby possibly impairing the operational flexibility of Georgian forces'[312]. While it seems beyond dispute that Georgia was exposed to cyber attacks, these cyber attacks were assessed from different angles. The Independent International Fact-Finding Mission on the Conflict in Georgia established by the European Union[313] focused on matters of attribution[314] and the novelty of cyber warfare[315] rather than questions of collective security and defence. However, since attribution is a challenge of an overarching nature, it will not be addressed here. By contrast, apparently convinced that attribution was possible in the Georgia case, U.S. Secretary of Defence Mr. Robert Gates has stated in a high level

310 Eneken Tikk *et al.*, International Cyber Incidents (2010), at 69.

311 For the sequence of events see e.g. Eneken Tikk *et al.*, International Cyber Incidents (2010), at 69sq and the September 2009 report of the Independent International Fact-Finding Mission on the Conflict in Georgia, Vol. II, at 218.

312 The September 2009 report of the Independent International Fact-Finding Mission on the Conflict in Georgia observes that some experts believe this (Vol. II, at 217sq).

313 Decision of the Council of the European Union dated 02 December 2008, OJ 2008 No. L 323/66.

314 According to the Report of the Independent International Fact-Finding Mission on the Conflict in Georgia (Vol. II, at 219), 'the nature of defence against cyber attacks at this stage of its development means that such attacks are easy to carry out, but difficult to prevent, and to attribute to a source'. For a detailed analysis of the origin of the cyber attacks on Georgia see Eneken Tikk *et al.*, International Cyber Incidents (2010), at 74sqq.

315 In discussing the (from its perspective: possible) integration of cyber warfare in the hostilities between Russia and Georgia the EU's Independent International Fact-Finding Mission on the Conflict in Georgia observed that, '[i]f these attacks were directed by a government or governments, it is likely that this form of warfare was used for the first time in an inter-state armed conflict'. Report of the Independent International Fact-Finding Mission on the Conflict in Georgia, Vol. II, at 219. It may be noted in this context that, given the absence of reciprocal force, the incident concerning Syria may not have amounted to an armed conflict despite its nature as a use of force which might have constituted an armed attack.

publication that: 'Russia's relatively crude - though brutally effective - conventional offensive in Georgia was augmented with a sophisticated cyber attack and well-coordinated propaganda campaign.'[316] The language used in this assessment seems to be carefully chosen; notably, the cyber attack faced by Georgia was not characterised as either enabling or multiplying the kinetic offensive; yet it was not merely addressed as a sustaining activity, either. As a result, the essence of this assessment may be that the elements carrying out the cyber attack may have been in a supporting rather than a supported role.

Too little is known about the 'short occasion of turbulence' in July 2008 to enable a compelling assessment of its nature from a collective security and defence perspective[317]. However, depending on the circumstances as well as the relevant strategy and doctrine, future 'occasions of turbulence' which affect NATO or one or more NATO Nations might create the impression that an entity acting from abroad is trying to test, or is actually testing, what effects is can generate using its cyber capabilities. If a NATO Nation were affected by such conduct, it would hardly overstretch the collective security mechanism established by Article 4 of the North Atlantic Treaty were it to request consultations with a view to obtaining military advice on the situation.

The Georgia example illustrates that the use of cyber technology may occur in support of a kinetic operation starting a campaign. The key question in this context is how non-enabling usages of cyber technology should be assessed from a legal and legal policy perspective, in particular if they occur prior to the first kinetic strike. One particular question deserving legal policy consensus would concern the circumstances in which 'the risk of a large-scale attack on NATO's command and control systems or energy grids'[318] can be considered to reflect that one or more of NATO's strategic competitors or potential adversaries possess cyber technology whose use can augment their kinetic capability. Information and intelligence regarding the circumstances as well as relevant strategy and doctrine may facilitate related assessments. However, it might nevertheless be more challenging to determine what augmenting usages of cyber technology justify pre-emptive / anticipatory self-defence or self-defence against an imminent attack than making the same determination with respect to enabling usages of cyber technology. At any event, the foregoing is without prejudice to the assessment that an ensemble of

316 Robert M. Gates 'The National Defense Strategy', in: Joint Forces Quarterly, issue 52, 1st quarter 2009, at 1/5.
317 According to reports, the website of the President of the Republic of Georgia was out of service for 24 hours, which may have been caused by a command and control server. See Eneken Tikk *et al.*, International Cyber Incidents (2010), at 69 for references.
318 Cf. the experts report at 45.

effects generated by the use of kinetic means as augmented by cyber technology would most likely cross the threshold of armed attack and hence trigger Article 5 of the North Atlantic Treaty.

The fourth type of scenarios covers the use of cyber capabilities on their own. The main challenge associated with this type of scenarios is tied to the objects affected in such cases, which will usually be civilian rather than military objects[319]. The example mentioned in the experts report concerning 'a large-scale attack on ⋯ energy grids'[320] (assuming for the purpose of analysis that energy supplies for the military are not affected thereby) as well as the cyber attack faced by Estonia in 2007 provide useful points of reference for this type of scenarios. The legal analysis regarding the cyber attack faced by Estonia in 2007 indicates that, from a collective security and defence perspective, this attack did not go beyond the level of a significant nuisance[321]. Even though Article 4 of the North Atlantic Treaty was not expressly invoked, NATO's collective security mechanism proved responsive; according to available reports, consultations were held and capabilities enabling a military assessment were made available. At the same time, the cyber attack faced by Estonia in 2007 as well as the risk of a future large-scale attack on energy grids should be the subject of contingency considerations since it may well be a precursor of what might yet be expected to come. Arguably, the fourth type of scenarios discussed in this paper bears the potential to create the biggest policy challenges NATO may have to tackle.

In a worst case scenario, future cyber attacks may deny one or more governments the ability to govern, or significantly interfere with democratic decision-making at all levels of society and government. For instance, a future cyber attack could significantly affect election results or policy choices. The recent history of the use of kinetic force has demonstrated that such effects may indeed occur[322]; the emergence of electronic government, which may sooner or later involve a 'cyberisation' of

319 Although the notion of 'military object' does not occur expressly in GP I, the differentiation between civilian objects (a notion used in Article 51(1) of GP I) and military objects is an underlying premise of its definition of military objective. Whilst a military object is always also a military objective since it will always fulfil the criteria set out in Article 52(2) of GP I, a civilian object only becomes a military objective if these criteria are met in an individual case.

320 Cf. the experts report at 45.

321 Reportedly, invoking Article 5 of the North Atlantic Treaty was never seriously considered. See Eneken Tikk *et al.*, International Cyber Incidents (2010), at 25sq.

322 The 11 March 2004 and the 07 July 2005 train bombs in Madrid and London, respectively, are ample proof that terrorists can affect the outcome of a general election or legislative priorities and decisions. Cf. my paper 'Air Policing and Counter-Renegade Action: Options beyond the German Aviation Security Act', 48 The Military Law and the Law of War Review 7 (2009) at 55 (text accompanying and footnote 86).

general elections[323], may be accompanied by additional vulnerabilities – which may materialise e.g. by way of identity theft coupled with subsequent use of the stolen identities in eVoting. Likewise, bringing down election servers designated for eVoting may effectively deprive a society of the ability to vote or the election outcome. All these hypothetical challenges have in common that they indicate what target a future cyber attack might be directed at, namely the integrity of the (democratic) decision-making process. Without such integrity, there may be serious doubts as to whether the exercise of the functions of government can still be considered 'effective' for the purpose of attributing relevant acts to any given State as its own sovereign acts[324]. In a similar manner, a future cyber attack could more or less sever the communication links within the government as well as between a government and the society it governs. For instance, interference with such areas of eGovernment as substitute online services for face to face interaction throughout of the administrative branches of various national governments may exploit the fact that sooner or later there will no longer be a workforce that could be mobilised and step in once the bulk of public services is performed based on the use of cyber technology. It may be argued that ultimately a cyber attack of that nature could severely affect the ability of a nation to maintain its political independence or otherwise push a state towards the edge of failure.

Developing a legal policy consensus regarding the best way to address such worst case scenarios from a collective security and defence perspective may require to double check certain well-established legal policy concepts[325]. The range of effects considered to indicate that an armed attack occurs in contemporary law of armed conflict – control of territory and sea access; death and injury; damage and destruction – might turn out to be too closely connected with the parameters of statehood in the 19th and 20th centuries, and hence require innovative adaptation to the realities of the 21st century. The UN Charter's prohibition of the use of force may be worthwhile revisiting for this purpose; namely, the protection of all nations' 'political independence' therein may see a renaissance as a result of a future legal policy discourse. One consideration guiding such discourse could be that it may

323 According to information received from CCD COE staff, Estonia has already introduced internet voting in local government elections. However, it might be worthwhile to not only think about Estonia's fairly advanced eGovernment but also identify equivalent vulnerabilities in other nations, thinking of e.g. the voting computers used in the U.S.

324 See my paper 'Air Policing and Counter-Renegade Action: Options beyond the German Aviation Security Act', 48 The Military Law and the Law of War Review 7 (2009) at 55sq (text accompanying and footnote 87).

325 One such concept is the differentiation between force and coercion for the purposes of applying Article 2(4) of the UN Charter. For a discussion see Matthew Hoisington, Cyberwarfare, the Use of Force & the Right of Self-Defence, 32 Boston College International and Comparative Law Review 439/447sqq (2009).

not make a significant difference whether a nation's political independence is degraded or denied by way of a cyber attack or by way of defeating its armed forces in a kinetic campaign. Ultimately, as Carl v. Clausewitz has observed, '[w]ar is ⋯ an act of force to compel our enemy to do *our will*.'[326] The opposite reverse holds equally true and is point-on in the present context. Within the Alliance, acts designed to impose a foreign actor's political will on a NATO Nation or its society may hence be considered amounting to acts of force – and may accordingly be qualified, for the purposes of international law, as a 'threat or use of force' resorted to in any State's 'international relations' or as an 'armed attack'.

A SPOTLIGHT ON CYBER THREATS CAUSED BY NON-GOVERNMENTAL ACTORS

When explaining the invocation of Article 5 of the North Atlantic Treaty following the 9/11 attack on the United States of America, the North Atlantic Council considered these attacks to possibly having been 'directed from abroad' rather than e.g. 'by another State'. In their reports to the UN Security Council under Article 51, multiple NATO Nations[327] – as well as Australia, following the invocation of the collective self-defence clause in the Security Treaty between Australia, New Zealand and the United States of America (ANZUS) dated 01 September 1951[328] by the Australian Prime Minister and U.S. President on 14 September 2001[329] – expressly mentioned Al Qaeda as one of the entities against which measures were taken in self-defence. No formal objections by members of the UN Security Council or otherwise by any State were reported at the time. This practice indicates that non-governmental actors may be considered responsible for an armed attack, and that self-defence may be directed against them.

Subsequently, questions were raised whether the notion of self-defence against

326 Carl v. Clausewitz, On War, translated by Michael Howard and Peter Paret and published by Alfred A. Knopf in the Everyman's Library series, New York - London - Toronto 1993, at Book One Chapter One Part 2 entitled "Definition" (my emphasis).

327 See the Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council (UN document S/2001/946); Letter dated 7 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (UN document S/2001/947); Letter dated 24 October 2001 from the Chargé d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council (UN document S/2001/1005); Letter dated 29 November 2001 from the Permanent Representative of Germany to the United Nations addressed to the President of the Security Council (UN document S/2001/1103).

328 Available at http://www.australianpolitics.com/foreign/anzus/anzus-treaty.shtml (last visited 03 August 2010).

329 Letter dated 23 November 2001 from the Permanent Representative of Australia to the United Nations addressed to the President of the Security Council (UN document S/2001/1103).

armed attacks carries an implicit limitation which would make the right of self-defence under Article 51 of the UN Charter available only in cases 'of armed attack by one State against another State'. However, the jurisprudence of the International Court of Justice which is usually referred to in support of this position[330] is not undisputed within the court itself. Justice Buergenthal has aptly observed that the majority of the court has taken a 'formalistic approach'[331] in the Advisory Opinion concerning the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory. In DRC v. Uganda, Justice Kooijmans has deplored that in failing to address the question of self-defence against activities of non-governmental actors, the Court 'has missed a chance to fine-tune the position it took 20 years ago' in the Nicaragua case[332], in which Justice Simma has joined him, adding that:

> Security Council resolutions 1368 (2001) and 1373 (2001) cannot but be read as affirmations of the view that large-scale attacks by non-State actors can qualify as "armed attacks" within the meaning of Article 51.[333]

Both Justices have alluded at possible changes of international law in light of practice and refined *opinio juris* in this context[334]. From a legal policy perspective, there is hence room to reinforce the post-9/11 development of practice and to consolidate the *opinio juris* thence refined. It may be noted that Advisory Opinions of the International Court of Justice are indicative rather than binding, and that the judgment in DRC v Uganda has binding force *inter partes* only. Accordingly, NATO and its Nations are not legally obligated to consider the jurisprudence discussed as binding upon them. As indicated by the Article 51 reports submitted in 2001, the perception among NATO nations of what amounts to an 'armed attack' may be broader than the approach taken by the International Court of Justice; nothing prevents them to maintain and reinforce this broader approach as a matter of policy. NATO and its Nations may hence consider it appropriate to take action in individual and collective against armed attacks perpetrated by non-governmental actors which are not attributable to a specific government, and they may consider it equally appropriate to contemplate taking such action against armed attacks perpetrated by non-governmental actors involving the use of cyber technology.

330 The most recent points of reference are the International Court of Justice's Advisory Opinion concerning the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory dated 09 July 2004, at para 139 and its judgment regarding the Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) dated 19 December 2005, at paras 146/147. In essence the ICJ concluded in both cases that activities of armed groups only trigger the right of self-defence if attributable to another State.

331 para 6 (p. 243)

332 Separate Opinion of Judge Kooijmans in DRC v. Uganda dated 19 December 2005, at para 25.

333 Separate Opinion of Judge Simma in DRC v. Uganda dated 19 December 2005, at paras 8 and 11, respectively.

334 Separate Opinions of Judge Kooijmans in DRC v. Uganda dated 19 December 2005, at para 25, and of Judge Simma in DRC v. Uganda dated 19 December 2005, at para 11.

CONCLUSION AD INTERIM: CYBER SECURITY AND DEFENCE FIT IN NATO'S SECURITY POLICY ACQUIS

Questions of attribution aside, the discussion the four different types of scenarios and the specific ramifications of cyber attacks perpetrated by non-governmental actors indicate that nothing in contemporary international law prevents NATO from both fully integrating cyber security and defence in its security policy *acquis* as well as taking appropriate action should the need to do so arise. However, considering also the challenges associated with the lack of a well-entrenched method, structure or process to harmonise the efforts of all relevant stakeholders, developing a solid legal policy consensus on matters of cyber security and defence may amount to a significant effort.

CONCLUSION

The demonstrated flexibility and consensus are fully capable of embracing NATO Nations' individual and collective cyber security and defence, as well. Unless otherwise decided, they may also come to bear with respect to NATO's approach to its own cyber security and defence – both in its Nations' territories and deployed. As demonstrated, the legal framework of the North Atlantic Treaty is sufficiently flexible to enable to Alliance to tackle cyber security and defence. However, as of yet the interpretation and application of the North Atlantic Treaty in cyber matters lacks the policy consensus needed to give a sustainable meaning to an(y) international agreement in its capacity as a policy document. In requiring the Alliance to start developing policy consensus concerning the interpretation and application of Articles 4 and 5 of the North Atlantic Treaty, the experts report 'NATO 2020: Assured Security; Dynamic Engagement' points in the right direction.

As far as the legal contribution to this consensus-building process is concerned, the types of scenarios discussed demonstrate the need for innovative analysis capable of challenging established conventional wisdom. Whilst, as indicated, all usages of cyber technology discussed seem to be eligible for integration in NATO's legal policy consensus concerning collective security and defence, their exact position therein would still have to be determined. This holds true both for legally nested policy development and decisions the Alliance may be called upon to take in the future. Moreover, forging a legal policy consensus on collective security and defence including questions of *jus ad bellum* might be facilitated by parallel concept and doctrine development as well as standardisation in a manner addressing related *jus*

in bello challenges[335]. Borrowing language from the experts report for the purposes of the present conclusion, the question of whether any of the usages of cyber technology discussed 'triggers the collective defence mechanisms of Article 5 [of the North Atlantic Treaty] … will have to be determined by the [North Atlantic Council] based on the nature, source, scope, and other aspects of the particular security challenge'[336].

335 Some of the examples contributing to the four types of scenarios discussed supra are reflected in the *jus in bello* considerations discussed by Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, 106 Michigan Law Review 1427-1451 (2008).

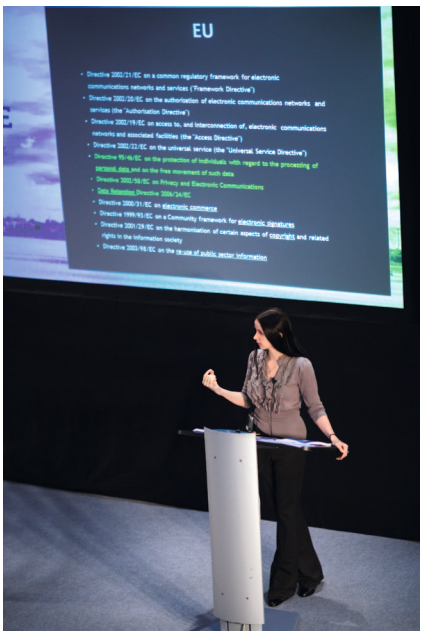
336 See the experts report, at 20.

AUTHOR AND CONFERENCE PHOTOS

↑ Dan Ryan, Professor of Systems Management at the National Defence University and Julie Ryan, Associate Professor and Chair of Engineering Management and Systems Engineering at the George Washington University sharing their thoughts with Jason Healy from Cyber Security Studies Association.

← Julie and Dan Ryan at the CCD COE Legal and Policy Conference 2009.

↑ Kadri Kaska and Anna-Maria Talihärm from the CCD COE Legal and Policy Branch.



↑ Peter Flory, Former NATO Assistant Secretary General (DI) and Chairman of the Cyber Defence Management Board, is discussing the Frameworks for Inter national Cyber Security (FICS) slides with Eneken Tikk.

← Eneken Tikk, the Head of the Legal and Policy Branch in CCD COE, introducing the concept of the Frameworks for International Cyber Security (FICS) and the relevant European Union regulation.

↑ Maeve Dion, Centre for Infrastructure Protection at Georg Mason University School of Law, is giving a presentation about public-private partnerships at the CCD COE Legal and Policy Conference 2009.

↑ Eneken Tikk, CCD COE, at the CCD COE Legal and Policy Conference 2009.

↑ Col Ilmar Tamm, the Director of CCD COE.

← Prof. Thomas Wingfield, George C. Marshall European Center for Security Studies.

↑ Estonian President H. E. Toomas Hendrik Ilves gave an opening speech at both the CCD COE Legal and Policy Conference 2009 and the CCD COE Conference on Cyber Conflict 2010.

↑ CCD COE Conference on Cyber Conflict 2010 was held on 15-18 June in the Estonian Drama Theatre and had altogether over 200 participants.

CONCLUSION

The year 2007, when the information systems of the Estonian government, electronic communication providers, banks and online media sustained large-scale cyber attacks, reinforced the need for interdisciplinary cyber security thinking not only for Estonia, but also on a wider international arena.

Past three years have drastically changed the global perception of cyber threats. Before the Estonian incident cyber security was regarded primarily as isolated risks and arrangements that organisations and national governments had to settle each for themselves. This fact made pre-2007 cyber security a sum of individual contingency plans having little to do with risks beyond everyone's own business interests and threats involved. Coordination of defences could be characterized as first and foremost driven by the incentive of developing uniform and standard solutions rather than an acknowledged necessity of concerted action.

Cyber attacks against Estonia were not unprecedented in terms of methods of attack and response. Instead, the Estonian chapter changed the way the international community understands and perceives cyber conflict by turning it from an „internal organisational or national matter" into an object of global attention and discussions.

Politically motivated cyber attacks have dragged experts and specialists out of their comfort zones and reassured the netizen society that there is a price to pay for an advanced information society and for the way of life they have chosen to lead.

Cases like Aurora, Conficker and Stuxnet remind us that cyber crime has not disappeared, but rather taken more sophisticated forms and expressions. Since 2007, politically and ideologically motivated attacks against information systems critical to the functionality of the society and state have been added to the earlier concept of cyber crime. Estonian lessons learned included amendments to the Penal Code which criminalized computer crime against critical information infrastructure as well as cyber terrorism.

Criminal policy adjustments are just one example of how different areas of policy and law need to be adapted to the new threat situation. In addition to cyber crime, national security relevant attacks test the limits of the existing legal framework of data protection, electronic communications and access to public information.

Furthermore, already today nations have started to develop cyber warfare capabilities and the occurrence of military attacks in cyberspace is just a matter of time.

In 2009, the aim of the Cyber Conflict Legal and Policy Conference organized by CCD COE was to map the most important legal areas influential to cyber security as well as the key problems from incident handling point of view. In the course of this Conference experts from 24 countries concluded that contemporary cyber threats can only be confronted when combining the regulation, remedies and legal practice of five key areas of law: law of network and information security (also referred to as cyber law or information society law dealing with, for example, data protection, e-commerce, electronic communications, access to information), criminal law (offences, investigation, cooperation), national security law and possible restrictions to human rights and liberties resulting from national security concerns, and finally Law of Armed Conflict.

In 2010 all these topics were followed up, focusing the discussion primarily on four problem areas: data exchange, state responsibility, criminal cooperation and the applicability of international law. Each of these problems was addressed by legal experts from at least two key areas involved (e.g. data exchange from cyber law and criminal law perspective, criminal cooperation from criminal law and national security law perspective etc.), the intent being to identify gaps between these areas of law and thereby come up with proposals on how to improve the existing legal framework.

From a theoretical perspective the information society is rich in nuances and offers different options for interpretation and implementation. Cyber law in action, as shown already by a few cases like Estonia, Lithuania, Georgia etc., differs to a great extent from theory. Therefore, despite the high level of expertise of the presenters, the discussions focused primarily on problems and challenges, instead of identifying concrete solutions.

In addition, several disagreements between legal and IT security experts were revealed during discussions about the applicability of law in general. The legal discussions tend to be difficult to follow for non-lawyers, which leads to the lack of contributions on the technical aspects of cyber incidents as well as real-life examples to illustrate the aspects of law and its implementation.

When analysing the reasons of this small "failure" and recalling that a similar situation has occurred over and over again in cyber security related legal conferences, a small group of legal and IT security experts came to the conclusion that on this level of discussions it is difficult if not impossible to reach conclusive solutions as

the discussion often tends to lack focus and in every single legal area the discussion without clear focus leads to more problems than solutions.

Already long before the national security dimension was added to cyber criminality, lawyers and IT security experts had disagreed about the quality and capability of cyber law – if and to what extent law should affect the "social contracts" governing the Internet and whether, due the architecture of the Internet, activities in this "global village" can be subjected to and enforced with legal concepts based on the principle of territoriality. One should keep in mind that in this debate, every legal expert has a background system – the legal principles governing the particular area of expertise, the area-specific definition package, scope of applicability and practice – which renders finding an agreement on if and to what extent the existing law is equipped to respond to cyber security concerns a challenging task.

Legal scholars, especially those focusing on the field of terrorism, national security or armed conflicts, often have little or no experience with technology. This fact does not encourage their communication with information security experts and regrettably hampers their understanding of how law is to be applied to a specific situation. Only with a principal understanding of the nature of a Denial-of-Service Attack or other types of cyber attack and their execution one can decide on the legal limits on Detection, Measurement, Disinfection & Defense.

The analysis group also observed that new legal practices have evolved in the course of international cyber incidents in 2007-2009 that were not reflected in sufficient detail in the presentations of the legal experts. Additionally, the presentations of lawyers having previously been engaged in the analysis of cyber incidents offered, from legal theory point of view, potentially disputable interpretations or did not consider potential pro- and counterarguments from other legal areas. It was therefore concluded that a more focused debate involving all four legal areas would be desirable.

The analysis group proposed that the legal discussion about cyber security could be more constructive if it comprised of the principles of all four legal areas, considered the issues and practice highlighted by cyber incidents and involved representatives with other fields of expertise concerning cyber incident handling (diplomacy, intelligence, military, politics etc.). The analysis group therefore proceeded to word the concept of 10 Rules: legal statements that are focused on issues as well as working solutions identified in the course of cyber incident handling or derive from debates around the subject matter.

10 RULES OF CYBER BEHAVIOR: THE CONCEPT

The 10 Rules concept is an attempt to provide more focus to the debate around legal issues related to cyber security and make these discussions easier to follow for legal experts with different professional background as well as for non-lawyers, thereby promoting an interdisciplinary approach to legal and practical aspects of cyber security. As a result of the discussions it is hoped that law can be better understood by decision-makers in the field of cyber security as well as the addressees of the regulation – be it nations, organizations or end users. It is also expected that the debate will broaden the analytical perspectives of legal scholars and give legal experts a better understanding about the links and interdependencies between different areas of legal expertise in order to avoid legal conclusions incompatible with the principles of military leadership or peculiarities of information architecture.

The concept frames simplified statements and conclusions from legal areas relevant to cyber incident handling and has emerged from the practice of handling international cyber incidents. The aim of the concept is to offer a more concentrated view on the different legal issues affecting the handling of cyber incidents and the level of cyber security in general. Additionally, the concept seeks to identify circumstances that either influence or might have an impact on legal practice and legislative drafting (e.g., the Estonian legal lessons learned from 2007 attacks).

The Concept also introduces legal lessons learned from recent incidents and thereby raises awareness about law implementation practices among lawyers. Hoping to constructively postpone international debates about new regulation needed, the 10 Rules Concept emphasizes the disparity between legal theory and practice, but also explains the "real life" context of cyber attacks to legal experts.

Considering that every rule has its own exceptions, prerequisites and restrictions for implementation, debate around the concept of 10 Rules should focus on different analogies, best practices and examples. Instead of "developing new issues", the discussions need to assess the practicality of the issues already identified and solutions to problems deemed practical.

In a nutshell, the concept proposes focusing international debate on the quality and interpretation of the existing law. In a longer perspective the debates are expected to provide ground for an interdisciplinary discussion about the need for new legal instruments. The analysis group takes the view that several issues considered as legal are, as a matter of fact, related to political or technical aspects and therefore need to be excluded from the list of legal issues or reconsidered from a constructive solution perspective (attribution, identification, even criminal cooperation). Also, several issues seen as challenges for the legislation can in reality

be solved by virtue of interpretation (neutrality) or demand simple exceptions from existing legal constructs instead of a wholly new legal approach (data protection, ISP liability). Only a constructive debate focusing on the quality of law can lead to a decision if and what issues need to be resolved by legislative initiatives.

The intent of the analysis group is also to emphasize the role of policy and social context around the interpretation and implementation of legal aspects. Therefore media, social networks and alternative regulation approaches (codes of conduct, best practices, code is law etc.) will be regarded as a supplementary framework for developing the rules. The project of 10 Rules is intended to combine the research and conclusions of different legal areas and generate interdisciplinary feedback, thereby supporting holistic and in-depth conclusions about the quality of existing law.

The main expectations related to the project include:

- Raised awareness about the legal issues of cyber security and ways to overcome them;
- Increased cooperation and coordination between areas of law as well as law and other expert areas related to cyber incident handling;
- Better understanding of the quality of law relevant to cyber incident handling;
- Well-grounded proposals for additional legislation on international level.

1. THE TERRITORIALITY RULE

Considering the global nature of cyber threats it is arguable whether territoriality-based legal frameworks can cope with the challenges that the concept of sovereignty poses to cyberspace. The lessons learned from Estonia, Georgia and other major cyber incidents show that nations are able to and need to make better practical use of the legal remedies and concepts available under national law by fine-tuning their national regulations.

Electronic communications, criminal sanctions, investigative authority, cooperation with Internet service providers and many other essential elements of successful cyber defense depend on the quality of the national law. Until the options for implementation and interpretation of national legal instruments in the current threat context are exhausted, it is difficult to conclude what, if any, additional remedies need to be discussed and agreed upon on international level.

Thus, the territoriality principle empowers nations to impose their sovereignty on information infrastructure located within their territory or otherwise subject

to their jurisdiction. By effectively updating their cyber security strategies and policies, nations will stretch the cyber security paradigm to cover cyber incidents threatening their national security.

The territoriality principle encourages nations to take as much advantage as possible of the existing jurisdictional structure. The responsibility of a state for securing its own networks is supported by internationally recognized concepts of non-intervention and sovereignty.

Every government can exercise effective control over the IT infrastructure located on its territory – such as ensuring the availability and quality of logs, having an overview of the providers of electronic communications, developing an understanding of threats and capabilities existing within its jurisdiction to cope with and manage the incidents and balancing the development of the information society with the interests of national security.

2. THE RESPONSIBILITY RULE

Nations, whose information infrastructure is used to launch abusive activities, need to consider the potential of being held responsible for the attacks. For example, in 2007, Estonian authorities accused Russia of cyber attacks launched against the Estonian governmental and critical private infrastructure networks. Russia has also been associated with the cyber attacks against Georgia (2008) and Lithuania (2008).

Similarly, China has been accused of launching cyber espionage attempts against the U.S. and other nations' information systems. In case of cross-border offences assistance is expected from countries, such as information leading to the identification of the source of attack, information about the perpetrators, methods and tools as well as search, seizure and investigation of the incident.

Also, countries may be expected to raise the level of their cyber security by establishing stronger control over the use and exploitation of the information architecture operated on their territory. Naturally, the balance between economic and security interests will be established on a case-by-case basis.

Legal constructs for attribution in case evidence of immediate involvement is lacking are known from, e.g., environmental law.

3. THE COOPERATION RULE

Due to the interconnectedness of the information infrastructure it is impossible for any nation to defend itself against cyber attacks without cooperating with States

whose infrastructure is used to route the attacks. Also, in the context of global cyber security threats and incidents, cooperation is needed between national governments and international organizations.

While the vast majority of the information infrastructure is claimed to be privately owned and operated, a significant dependence exists on public information services and networks that the private sector supports on contractual basis. Cooperation may be needed in the form of consulting, information exchange, reallocation of resources, but also supporting services under attack. The cooperation rule is therefore common sense for the coordination between public and private sector as well as for resolving cross-border incidents.

National provisions on Internet service provider cooperation, data exchange and partnerships as well as coalition agreements will support the legal framework for cooperation.

4. THE SELF-DEFENSE RULE

Self-defense is a concept known in both criminal and international law. In principle, everyone has the right for self-defense whilst taking into account the limitations as regards the proportionality and necessity of such action.

From criminal law point of view, acting in self-defense will exclude liability for an otherwise wrongful act. Criminal law allows for the use of defense anytime the victim reasonably believes that unlawful force is about to be used against him. This is not to say that every "hack-back" can be justified under the concept of self-defense, but rather, this legal concept is seen as a last resort remedy for the one attacked.

On international level, the legal criteria for invoking individual and collective self-defense are established under customary law as well as provided for in the UN charter and international case law. A cyber attack invokes individual and collective self-defense if it rises to the threshold of an "armed attack". The assessment of whether a cyber attacks by its effect, consequences or nature is equivalent to an armed attack will be made by national authorities, and in case of a request for collective action, also by international partners (e.g., by the North Atlantic Council for invoking Article 5 of the NATO Treaty).

So far, no cyber attack has crossed this threshold and consequently, no military response has been given to a cyber attack to date. From a legal point of view a kinetic response in self-defense against a cyber attack can be permissible provided that it is necessary to achieve the aim of the act (putting an end to the attack) and

that the counter-attack is proportionate considering the method and effect of the aggression.

5. THE DATA PROTECTION RULE

The balance between network monitoring and information exchange necessity needs to be carefully assessed against the individuals' right to privacy. Currently, a considerable divide exists between the legal and technical approach to data and its security. While monitoring network data seems to be a well-established and routine activity in technical communities, it raises significant concerns among the legal experts.

According to the EU Data Protection Directive, any information relating to an identified or identifiable natural person is regarded as personal data. The prevalent opinion in the countries implementing the EU Data Protection Directive is that IP addresses are to be regarded personal data and therefore subject to processing restrictions under national legislation.

Such restrictions include the requirement of the consent of the data subject for processing this data, prohibition to transfer this data to third countries as well as potential inadmissibility as evidence of such data obtained in an unlawful manner.

There are ways to work around these prohibitions on national level. The Directive allows for exceptions in the interests of public interest and national security. Also, exceptions are applied to data protection requirements in the interests of criminal proceedings. Clearly identifying the need for and means of data and packet inspection will help establish a desirable balance between privacy and monitoring.

6. THE DUTY OF CARE RULE

The concept of duty of care is well known in many areas of law: one is under an obligation to guarantee the protection of personal data processed by him or her, rules also apply with regard to consumers and information society service users.

Under the EU Data Protection Directive controller of personal data must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and

the nature of the data to be protected.

As cyber threats of political context become more prevalent, the duty of care concept can be extended to develop security standards for critical information infrastructure and governmental or military information services.

7. THE EARLY WARNING RULE

In 2008, 300 Lithuanian websites got defaced with the "sickle and hammer" symbol after the Lithuanian Parliament had passed a law that banned, inter alia, the use of Soviet symbols. Despite the fact that a single ISP vulnerability was exploited to deface the websites, this case brought up a legal construct and introduced a trend, which, if implemented widely, could considerably improve the cyber security situation.

Namely, the Lithuanian ISP, having found out about the upcoming attacks, issued an early warning to its customers and informed them about the incident.

The fact that Lithuanian governmental agencies were informed of the attacks beforehand raises the issue of the standard of service level agreements (SLAs) for governmental information infrastructure, as well as considerations for the necessity for defining a non-discrimination duty to ensure that both public and private sector ISP-s and web hosts be warned about known threats.

The issue of SLAs is, to a great extent, a matter of national legislation or contracts. For Lithuania as well as other European Union members, the obligations of the service providers in ensuring security of services derive from the ePrivacy Directive EC/2002/58.The ePrivacy directive foresees a general obligation for the service provider to take appropriate technical and organizational measures to safeguard the security of its services. If necessary (with respect to the security of the network upon which the service provider's services are provided), the service provider must coordinate further actions with the provider of the public communications network to which it is connected.

8. THE ACCESS TO INFORMATION RULE

Unless provided for otherwise, public sector information is perceived to be publicly accessible. The transparency of governmental acts and records is a strong legal trend in Europe, giving the public the right to be informed about threats and decisions related to their life and well-being.

While, on the one hand, access to information is a vehicle for the public to find out

about threats and attacks and thereby raising awareness about cyber security, it also may result in unwanted publicity.

A natural conflict exists in the private sector incentives to make public the fact of cyber attacks against them as well as the effect of the attacks as it might reduce trust against their business model or services. Politically motivated cyber attacks often require the publication of related facts. A balance therefore needs to be created between the public and private sector interests.

Also, publicly discussing the details of the methods, targets and effects of the attack may result in increased vulnerability as such publication carries information that the attackers would not know otherwise.

Therefore the legal framework of access to information will be an important field for cyber security from strategic communication and awareness point of view.

9. THE CRIMINALITY RULE

The criminality rule serves as a reminder rather than something qualitatively new. It is well established in criminal law that cyber attacks can only be investigated and prosecuted under criminal law if those acts are qualified as criminal offenses.

It is therefore practically impossible to impose State coercion on anyone engaged in a cyber attack unless the specific activity and/or consequence has been listed as a crime under national law. Politically motivated cyber crime is more dangerous to the society in general than it is to any specific person or entity and thus may require a different approach on national level than economically motivated cyber crimes.

The Lithuanian case proved that as a result of political tensions, random private sector targets might come under a cyber attack. The Estonian case demonstrated that in a country with a rather low rate of cyber criminality, politically motivated DDoS attacks can effectively disrupt the communication within and with the government and leave national law enforcement agencies empty-handed even with sufficient investigatory powers within their own jurisdiction. In the Georgian case we saw how seamless connections between patriotic hackers and their war-waging government almost effectively contribute to kinetic warfare, but nevertheless go without effective legal remedies.

Existing international agreements, such as the Council of Europe Convention on Cybercrime, are a good start for enhancing and harmonizing national legal responses to cyber crime.

10. THE MANDATE RULE

The mandate rule is relevant for defining and coordinating international efforts of global cyber security. This issue gains practical importance especially from the perspective of developing or revising existing cyber security agendas.

To justify governmental "investments" in their cyber capabilities, international organizations should make use of and enhance efforts undertaken by other entities. While NATO's primary focus in the field could be related to collective self-defense procedures, the organization still needs an agenda for handling cyber incidents below the threshold of a "cyber armed attack", targeted both against the organization itself and the individual Allies. Prior to deciding which measures need to be put in place between the Allies for defending against an incident, it is necessary to understand the already existing framework in order to avoid conflicting practices and gaps in coordination.

For example, international cyber crime harmonization has been in the focus of at least six major international organizations. For states party to a number of international organizations, the question of what is the input of every organization to national cyber security framework ultimately arises.

Cyber defense is times and times more costly than a cyber attack and over time, as governmental information infrastructure becomes more often a target, developing national and international capabilities will become an investment issue. Therefore, the niche for NATO could be gathering, exchanging and developing best practices in the field of cyber attacks of national security relevance and the aspects of cooperative defense and security.

WAY AHEAD

In 2011 we expect to follow up the 2010 Conference and the Rules Concept in a number of workshops each focusing on one or two rules and engaging specialists from respective legal, technology and policy areas. Also, the concept will be developed further in a group of experts and everyone who is interested in participating in this process is more than welcome to join!

INTERNATIONAL CYBER SECURITY

LEGAL & POLICY PROCEEDINGS

2010

Contact & feedback
publications@ccdcoe.org

ISBN 978-9949-9040-4-4