THE TALLINN PAPERS

A NATO CCD COE Publication on Strategic Cyber Security

JEFFREY CARR

RESPONSIBLE ATTRIBUTION: A PREREQUISITE FOR ACCOUNTABILITY

Tallinn Paper No. 6
2014

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Previously in This Series

No. 1 Kenneth Geers "Pandemonium: Nation States, National Security, and the Internet" (2014)

No. 2 Liis Vihul "The Liability of Software Manufacturers for Defective Products" (2014)

No. 3 Hannes Krause "NATO on Its Way Towards a Comfort Zone in Cyber Defence" (2014)

No. 4 Liina Areng "Lilliputian States in Digital Affairs and Cyber Security" (2014)

No. 5 Michael N. Schmitt and Liis Vihul "The Nature of International Law Cyber Norms" (2014)

Roles and Responsibilities in Cyberspace

The theme of the 2014 Tallinn Papers is 'Roles and Responsibilities in Cyberspace'. Strategic developments in cyber security have often been frustrated by role assignment, whether in a domestic or international setting. The difficulty extends well beyond the formal distribution of roles and responsibilities between organisations and agencies. Ascertaining appropriate roles and responsibilities is also a matter of creating an architecture that is responsive to the peculiar challenges of cyberspace and that best effectuates strategies that have been devised to address them.

The 2014 Tallinn Papers address the issue from a variety of perspectives. Some of the articles tackle broad strategic questions like deliberating on the stance NATO should adopt in cyberspace matters, or exploring the role small states can play in this domain. Others touch upon narrower topics, such as the right to privacy in the growingly intrusive national security context and whether software manufacturers should be compelled to bear their burden of cyber security by making them liable for faulty software. The thread running through all the papers, however, is their future-looking approach, one designed to inspire discussion and undergird strategic development.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

Responsible Attribution: A Prerequisite for Accountability

Jeffrey Carr[1]

"Master Li, how are we going to murder a man who laughs at axes?" I asked.

"We are going to experiment, dear boy. Our first order of business will be to find a deranged alchemist, which should not be very difficult. China," said Master Li, "is overstocked with deranged alchemists."

Barry Hughart, *Bridge of Birds: A Novel of an Ancient China That Never Was*

Attribution in cyberspace remains an ongoing challenge due to a series of complicating factors such as the ability of an unknown aggressor to mimic the tools, techniques, and procedures of a better-known aggressor with whom the target already has tense relations. Yet another complication is an over-reliance upon signals intelligence (SIGINT) without physical corroboration through human intelligence (HUMINT). Then there is the matter of an insecure global network, which unfortunately is considered by many to be an asset. Intelligence agencies prefer weak encryption standards to strong because the former are easier to break. Privacy advocates fight for the right to be anonymous on the internet, which includes masking not only one's identity but one's location as well. Internet Service Providers (ISPs), like the telephone companies before them, do not want to be held responsible for what is transmitted across their networks, nor do they insist on verification of identity before leasing server time to their customers: they would lose millions of dollars in revenue if they did.

As long as the infrastructure upon which attribution relies is insecure, and while both private companies and government agencies have a vested interest in keeping it that way, states will continue to struggle with the challenge of knowing who to hold responsible in the event that a digital attack is carried out that has significant enough effects to cross the legal threshold governing the right of self-defence – if planes start colliding in mid-air and the Secretary of Defense wants to mobilise for war.

1 Founder of the Suits and Spooks security forum; President/CEO of Taia Global, Inc.

It Depends on What Is Meant by "Attribution"

Attribution is made difficult by the myriad ways in which the problem has been defined, denied, diminished, dissected, and even commercialised. Below are a few examples of well-known commentators who believe that the attribution process has either already been solved, or is on its way to being solved:

> *"Sophisticated adversaries will take steps to obfuscate their true location and identity through the use of proxy systems, whether they are compromised computers or anonymization services or both. Despite these precautions, trace back techniques and digital forensics can provide the technical means to allow the attackers to be discovered."*[2] – Robert Knake (2010)

> *"Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America."*[3] – U.S. Secretary of Defense Leon Panetta (2012)

> *"The good news is that there has been a revolution in our ability to identify cyberspies. It turns out that the same human flaws that make it nearly impossible to completely secure our networks are at work in our attackers too."*[4] – Stewart Baker (2013)

> *"For national security policymakers, knowing "who is to blame?" can be more important than "who did it?" Moreover, attribution becomes far more tractable when approached as a top-down policy issue with nations held responsible for major attacks originating from their territory or conducted by their citizens."*[5] – Jason Healey (2012)

> *"Online attribution only gets easier as time passes. Fewer and fewer people lack an online presence, making it easier to identify them later."*[6] – Richard Bejtlich (2013)

---

2 Prepared statement by Robert K. Knake, International Affairs Fellow, Council on Foreign Relations, before the Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives, 2nd Session, 111th Congress on 15 July 2010, available at: http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57603/html/CHRG-111hhrg57603.htm.

3 Remarks by Leon Panetta, U.S. Secretary of Defense, on Cybersecurity to the Business Executives for National Security, New York City on 11 October 2012, available at: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

4 Stewart Baker, formerly General Counsel, National Security Agency and Assistant Secretary for Policy, Department of Homeland Security, 'The Attribution Revolution: A five-point plan to cripple foreign cyberattacks on the United States,' *Foreign Policy* (17 June 2013).

5 Jason Healey, Director, Cyber Statecraft Initiative, Atlantic Council, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks,' Atlantic Council Issue Brief (January 2012), available at: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.

6 Richard Bejtlich, then Chief Security Officer, Mandiant, Twitter message (28 August 2013), available at: https://twitter.com/taosecurity/status/372851873491218433.

All of those quotations are problematic for reasons that this paper will explore. The ease or difficulty of attribution is determined in large part by the attackers themselves. For example, the FBI, in cooperation with various foreign counterparts, has been successful in catching many members of the Anonymous collective who were allegedly involved in criminal acts in cyberspace. However, members of Anonymous have never shown the capability to launch anything more sophisticated than a 15-year-old SQL injection attack or using automated Denial of Service tools to disrupt traffic to websites. Mandiant, the cyber security company that received international attention for its APT1 report on a Chinese PLA unit allegedly involved in thousands of cyber espionage attacks, acknowledged that "attacker blunders" and "sloppy operational security" were responsible for at least some of its findings.[7]

Training, tools, budgets, professionalism and sheer guesswork may all play a part in whether any attempt at attribution will be successful or not. This paper will grant that attribution is straightforward for low-hanging fruit like amateur hacktivists or bored Chinese soldiers with inadequate operational security. Instead, it will examine the challenge of assigning attribution when a skilled, disciplined, and well-funded team of state or non-state actors has launched a cyber attack of significance, such as one potentially causing long-term serious damage to a nation's power, water, banking or transportation systems. Any government that experiences such an attack has, at the very least, a moral obligation to its citizens to track down and punish those responsible; but no response, legal or otherwise, can be forthcoming unless or until the aggressor is identified. That said, identifying the aggressor is complicated by a number of factors.

Complicating Factor No. 1

A cyber attack mounted against critical infrastructure which results in serious damage and accumulates nth level effects (chaos, looting, rioting, etc.) with human casualties can be carried out in an entirely covert manner without being part of a corresponding kinetic attack or military operation.

In the recent past, military operations (e.g., 2002 Russian-Chechen war; 2007 Israeli strike against Syria; 2008 Russian invasion of Georgia; 2009 Israel's Operation Cast Lead; 2014 Israeli-Hamas war: 2014 Russia-Ukraine conflict) have

7 Intel Team, 'Threat Actor Tactics and Targeting Predictions for 2014,' *Mandiant M-unition blog* (23 December 2013), available at: https://www.mandiant.com/blog/threat-actor-tactic-targeting-predictions-2014/.

been accompanied by cyber attacks, making the attribution problem relatively moot. Stuxnet, on the other hand, was a stealth attack and while attribution by intuition laid the blame either on the U.S. or Israel or both, there was no hard evidence until the White House initiated multiple leak investigations,[8] validating journalist David Sanger's identifying claims made in his 2012 book on U.S. clandestine operations and the accompanying *New York Times* articles.[9]

If no overt hostilities or geopolitical tension exist between the victim of a cyber attack and the attacker, the victimised government must rely on its security and intelligence services to discover the responsible actor.

It is neither sufficient nor legally justifiable to simply trace an attack to a server located in a foreign country. This has been acknowledged in Rule 8 of the *Tallinn Manual*, which states that "the fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State."[10]

Complicating Factor No. 2

A cyber attack may be timed to take advantage of geopolitical tensions between two adversary states by an unknown third state or non-state actor.

It is quite easy to take over a computer in a government office and convert it to a command and control server, especially if one of the two states that is being manipulated has many of its nation's computers already compromised by malware.[11] This tactic would be even more effective if conducted during a time of interstate hostility or even diplomatic tension, when hasty assumptions about attribution would be almost impossible to avoid.

8 Kim Zetter, 'Sen. Feinstein Calls for Hearing on Stuxnet Leaks as FBI Begins Probe,' *Wired* (6 June 2012).

9 David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran,' *The New York Times* (1 June 2012).

10 *Tallinn Manual on the International Law Applicable to Cyber Warfare* [hereinafter *Tallinn Manual*], gen. ed. Michael N. Schmitt (New York: Cambridge University Press, 2013), r. 8.

11 'In January, 50 per cent of computers scanned by Panda ActiveScan worldwide were infected with some type of computer threat,' Panda Security (8 February 2011), available at: http://www.pandasecurity.com/mediacenter/press-releases/in-january-50-percent-of-computers-worldwide-were-infected-with-some-type-of-computer-threat/.

Complicating Factor No. 3

Much of what is presumed to be known about cyber threat actors originates from the private sector and is based almost solely upon common technical indicators[12] *rather than first-person knowledge gained from human intelligence operations or criminal prosecutions.*

The process that private cyber security firms use to identify and name cyber threat actors is arbitrary and lacks any centralised oversight or validation:

> *"Overall, the key findings indicate that organizations use a diverse array of approaches to perform cyber intelligence. They do not adhere to any universal standard for establishing and running a cyber intelligence program, gathering data, or training analysts to interpret the data and communicate findings and performance measures to leadership."*[13]

In fact, names like Comment Crew, APT1, Soy Sauce, GIF89a, Shanghai Group, and Comment Panda all represent the same "group"; a group that may or may not actually exist as a hacker organisation or military unit.[14] Even if it does, no one knows who the members are (with a handful of notable exceptions[15]), or whether they have moved on to other groups. Hundreds of such made-up monikers have been created and no one knows if they represent actual groups, duplicates of other groups, or the product of overly presumptive cyber security companies competing with one another to sell cyber security intelligence. Some of the classified cables which surfaced during the Wikileaks revelations contained much of the same information that was previously shared by cyber security companies in public press releases and unclassified reports. This suggests that at least some of the classified threat intelligence that the U.S. Government has on Chinese hackers originated from the private sector, ostensibly with no oversight

12 FireEye, 'Digital Bread Crumbs: Seven Clues To identifying Who's Behind advanced Cyber Attacks' (2014), available at: https://www.fireeye.com/resources/pdfs/digital-bread-crumbs.pdf. This white paper serves as one example of how assigned names like APT1 or Comment Crew do not refer to actual groups but to a grouping of technical indicators held in common by those responsible for any given attack.

13 Troy Townsend et. al., 'SEI Innovation Center Report: Cyber Intelligence Tradecraft Project. Summary of Key Findings,' Software Engineering Institute, Carnegie Mellon (January 2013), available at: http://cyberunited.com/wp-content/uploads/2013/03/Cyber-Intelligence-Tradecraft-Project.pdf.

14 Mandiant's APT1 report claims to have positively identified APT1 as People's Liberation Army Unit 61398, however, there has been no independent verification of that claim and other security researchers including this author have found numerous factual errors and faulty analysis in the report. For the report, see Mandiant, 'APT1: Exposing One of China's Cyber Espionage Units,' available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

15 Michael Riley, Dune Lawrence, 'UglyGorilla Hacker Left Tracks, U.S. Cyber-Hunters Say,' *Bloomberg* (22 May 2014).

and little to no source validation.

In the aftermath of a disruptive cyber attack, when the President asks his National Security Advisor and the heads of his intelligence agencies to identify who was responsible, the quality of the intelligence analysis that he receives will depend on the quality of the source material collected. The current state of commercial cyber threat intelligence collection and analysis is woefully inadequate in that regard. If the duplication of that inadequate material is absorbed into the classified analyses of the state's intelligence organs, there may be reason to doubt what the intelligence community knows and does not know about state and non-state cyber threat actors.

Complicating Factor No. 4

It no longer requires a nation state's resources and several years' work to develop a Stuxnet-like cyber weapon.

When Stuxnet was developed in 2007 or 2008, it took several years and millions of dollars to create, and the malware succeeded in destroying just under 1,000 of Iran's nuclear enrichment centrifuges at Natanz. In 2012, Shamoon was created by one or more hackers of moderate skill who tried to reverse-engineer the Wiper virus allegedly created by the same lab which created Stuxnet.[16] It destroyed 2,000 servers and 32,000 workstations at Saudi Arabia's national oil company Saudi Aramco, thereby impacting its business operations for weeks. It is important to note that it was relatively easy for the hackers to modify the malware developed by a state, which complicated any future technical analysis. Think of an unregistered gun which may be used by one person to commit a crime and is then left on the street for someone else to pick up and use in a different crime, and so on. Malicious code is used in a similar fashion, in that the author of the code may be entirely unrelated to the person who subsequently uses or modifies the code for an attack.

The skill level of computer hackers increases many times faster than the technology that they dissect while looking for vulnerabilities. One can no longer assume that an attack with potentially harmful and disruptive consequences is only within the province of a nation state or well-funded group. Rather, it could today be the work of one person located anywhere in the world. This complicates the process of attributing an attack to the responsible party almost to the point of impossibility.

16 On Shamoon, see, e.g., Nicole Perlroth, 'In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back,' *The New York Times* (23 October 2012).

Attribute with Caution

The attribution of an attack which is destructive enough to justify the victim's response with force in self-defence must be done in accordance with international law and must reach a high threshold of certainty.[17] The digital forensic evidence collected should certainly be shared with other nations' CERT teams for peer review to avoid confirmation bias. While cyber attacks can be traced to infrastructure located within another state's borders, that fact alone is not enough to justify a counter-attack. Other possibilities such as the remote control of servers in another state must also be ruled out.[18] Even if the server used was connected to another state's government network, "it is not sufficient evidence for attributing the operation to that State."[19]

With respect to the technical challenges of attribution, it is important to note that the advance planning for a computer network attack of this magnitude would involve multiple servers across multiple countries. The attackers would likely also be careful to set up one or more shell businesses with corresponding servers in nations other than their own so that, even if an IP-address could be traced back through multiple hops, its originating source would still not be located in the state that planned and executed the attack. This type of operational security is used by at least one industrial espionage group in China, according to the FBI.[20]

Unfortunately, the rapid adoption of insecure technologies running critical infrastructure will not be stopped. As the world becomes more digitally connected, it also becomes easier for adversaries to cross physical, financial, and technological barriers that historically have made it difficult or impossible to cause harm in an anonymous manner. However, in today's global economy, it is highly unlikely that any developed country in the G8 or G20 would attempt to

17 International law does not explicitly dictate the level of certainty the target state needs to possess in order to take action in self-defence. However, some states, such as the United Kingdom and the Netherlands, have indicated that it is a high threshold. See 'Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13' (22 March 2013), available at: http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm; 'Government response to the AIV/CAVV report on cyber warfare,' available at: http://www.aiv-advies.nl/ContentSuite/template/aiv/adv/collection_single.asp?id=1942&adv_id=3016&page=regeringsreacties&language=UK.

18 *Tallinn Manual, supra* note 10, r. 8.

19 *Ibid*., r. 7.

20 Criminal complaint in the case of *United States of America v Su Bin* (27 June 2014), available at: http://online.wsj.com/public/resources/documents/chinahackcomplaint0711.pdf.

take down another nation's banking, power, or transportation system because it would serve more as a collective punishment than anything else.

The most likely adversary responsible for a covert attack against those critical systems is an extremist group (religious, political, or anarchist), and the best way to learn which of those groups may have been responsible post-attack is to already have in place a long-term counter-intelligence campaign of infiltration and the development of trusted contacts with access. This cannot be done virtually or from behind a computer. Rather, those intelligence agencies that have yet to devote the bulk of their budget to signals capabilities may be best positioned to tackle the problem of attribution. They understand the need to continue to fund and even expand human intelligence – this is still vital, despite the fact that we are living in the age of Facebook, Twitter and Instagram.