Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Sanjay Goel, *Connections QJ* 19, no. 1 (2020): 87-95
https://doi.org/10.11610/Connections.19.1.08

Research Article

How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race

Sanjay Goel

New York State Center for Information Forensics and Assurance, University at Albany, 1400 Washington Avenue, Albany, NY 12222

https://www.albany.edu/cifa/

Abstract: Cyber warfare is a critical component of nation-states' military arsenals, and a cyber arms race has emerged in the absence of international agreements (norms and confidence-building measures) to limit the use of cyber warfare. One key impediment to building consensus on cyber norms and confidence-building measures is a lack of transparency in cyber weapons development and poor attribution of attack perpetrators. Recently, there has been an improvement in attribution capabilities based on better data collection and the profiling of known hackers and nation states by intelligence agencies, and this should give impetus to efforts to establish confidence-building measures and cyber norms. This article discusses the need for and challenges associated with attribution, recent advances that will lead to better attribution, and the collective responsibility of nation states in addressing these challenges. It suggests several initiatives to reduce chances of cyber conflict, as well as to prevent cyber conflicts from escalating, such as defining clear processes for attribution, creating neutral bodies for incident analysis, and limiting the scope of retaliation based on the confidence in attribution.

Keywords: cyber warfare, cyber arms race, attribution, confidence-building.

Introduction

The prevalence and risk of cyberattacks continue to rise in parallel with our increasing reliance on the Internet for systems of economic production, supply and distribution chains, finance, power, transportation, and other critical infrastruc-

tures. Cyber warfare is becoming the next serious threat to national security [1] that can impact not only life and property but also financial markets.[2] According to the Centre for Strategic and International Studies (CSIS), the total number of cyber-attacks against government agencies, defense and high-tech companies, or economic crimes with losses of over one million dollars rose from 21 in 2014 to 58 in 2017.[3] This CSIS list, built on open-source data only, depicts a worrisome trend of rising cyberattacks attributed to state-sponsored groups acting against the political or economic interests of other states.

In testimony delivered to the US Armed Services Committee in January 2017, James Clapper, former US Director of National Intelligence, stated that more than 30 nations were developing offensive cyberattack capabilities as of late 2016. He further opined that "the proliferation of cyber capabilities coupled with new warfighting technologies will increase the incidence of standoff and remote operations, especially in the initial stages of conflict."[4] As policymakers warn of the dangers of cyber conflicts and exalt the virtues of cyber peace, most states consider cyberspace the fifth operational domain, with equal, or perhaps greater future importance to the traditional domains of land, sea, air, and space. State military and intelligence agencies continue to conduct cyber espionage and covert attacks on computer systems and networks in pursuit of strategic political or military objectives, both before and during conflicts. Yet, there is limited transparency on how states consider using their cyber capabilities, as only a few countries have publicly announced their cyber doctrines and underlying strategies. For example, McAfee, the global computer security software company, estimated in 2007 that over 120 countries were working on cyber commands,[5] whereas Dévai listed 114 countries that, as of 2013, were developing civilian and military cyber capabilities, policies, doctrines and organizations at varying levels of maturity or focus.[6] Considering that many of the officially declared 'defensive'

---

1 Richard A. Clarke and Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It* (New York, NY: Harper Collins, 2010).

2 Sanjay Goel and Hany A. Shawky, "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information & Management* 46, no. 7 (October 2009): 404-410, https://doi.org/10.1016/j.im.2009.06.005.

3 Centre for Strategic and International Studies, "Significant Cyber Incidents Since 2006," 2018, accessed June 20, 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf.

4 James R. Clapper, Marcel Lettre, and Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee 'Foreign Cyber Threats to the United States'," January 5, 2017, accessed June 14, 2018, https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

5 Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," *Air Force Law Review* 64 (2009): 121-173.

6 Dóra Dévai, "Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions," *Academic and Applied Research in Military and Public Management Science (AARMS)* 15, no. 1 (2016): 61-73, https://folyoiratok.uni-nke.hu/document/uni-nke-hu/aarms-2016-1-devai.original.pdf.

cyber capabilities could easily be deployed in offensive cyber operations, as well as the fact that data assembled by cyber experts is often based on publicly available information only, it is not surprising that such estimations vary, and that the true state of cyber warfare preparedness and capabilities worldwide is difficult to ascertain. This high degree of uncertainty, when coupled with the low cost and easy acquisition of cyber weapons, ample and growing target selection, and multiplicity of types of attacks that may go unnoticed for a long time, contributes to a prevailing state of cyber insecurity in the international community. The problem is further exacerbated by the fact that there is no commonly accepted terminology of critical cyber terms (e.g., 'cyber' vs. 'information' security) among key cyber actors, which affects the ability of most likely strategic adversaries to establish common ground as a prerequisite for dialogue.

Cyber warfare is a broad term that refers to actions by nation-state actors (or other international organizations with *mala fide* intentions) to use hacking tools to achieve military objectives in another country. The tools for hacking are varied and can include malicious software, denial-of-service attacks, social engineering, fake news, and malicious insiders as well as tools for camouflaging identify of hackers or misdirecting attribution. The objectives could be tactical or strategic. The tactical objectives could be degrading the capability of an adversary both in the battlefield or in weapons development (e.g., Stuxnet) or espionage to collect intelligence. The strategic objectives could be the use of soft power such as propaganda to influence public opinion for regime change or altering the political outcomes of the election or hard power by leaving dormant malicious software in critical infrastructure to leverage during times of conflict.

The boundary between conventional and cyber war is blurring as conventional defensive and offensive capabilities increasingly use the Internet for command, control, communications, and intelligence, making information and communication infrastructures and networks both the targets and vehicles of military attacks. At the same time, the Internet has become the communications backbone required for the functioning of modern societies and economic systems. Therefore, the nature and means of the military defense of these systems also have to change and become more flexible to adapt to these emerging threats. Above all, the nascent cyber defense mechanism of any state must be able to provide the national political leadership with answers regarding a number of critical questions: What is the origin of a cyberattack; where did it come from? Who is responsible? What is the recommended course of action, or response?

Attribution

Attribution of cyberattacks is very important, especially to justify retaliatory actions against the perpetrators and prevent accidental retaliation against innocent targets. The entire domain of cyber norms and confidence-building measures is centered on visibility, i.e., being able to identify perpetrators of attacks and being able to ascertain adversarial strength. In the absence of such

verification, the suspicion remains, and nation states assume the worst and prepare themselves by building stronger and stronger arsenals to maintain strategic equilibrium.

Anonymity is often regarded as a key foundational principle of the Internet, driven by the need to shield the identity of the user and dissociate users' actions from their identity.[7] Such anonymity ensures the ability to speak freely without fear of retribution, which can be beneficial in political commentaries, debating contentious issues, asking personal questions, researching competitors, and purchasing goods or services without revealing personal choices. Privacy advocates have gone to great lengths to protect the anonymity of users by providing services, such as remailers and encryption, that further camouflage users' identities and protect them from government surveillance. However, while beneficial in some contexts and circumstances, such anonymity also shields the perpetrators of crime and terrorism on the Internet.[8] The cloak of anonymity protects and enables perpetrators of money laundering, extortion, espionage, and theft. Similarly, actors engaging in cyber warfare leverage anonymity on the Internet to conduct surveillance, probes, and attacks without drawing attention to their actions. There has to be a balance between anonymity and security to ensure people's right to privacy and security.[9]

Forensics and Attribution

Despite the inherent anonymity of the Internet, users leave traces of their activities along the way. These traces can provide valuable clues that can reveal the identity of the attackers and their possible motivations. The goal of digital forensics is to collect the traces, connect the dots, and make inferences about the incident, including identifying the perpetrators, determining the mechanism of operation, and cataloging the information compromised or altered. The tools, processes, and knowledge for digital forensics are freely available. Still, the anonymity of the Internet makes such analysis difficult, especially in the case of cyber warfare, where relevant information of the attack is hidden behind country firewalls and protected by the sponsors of the attack.

Digital forensics can strip away some of the Internet's anonymity and narrow down the field of perpetrators by piecing these clues together and creating a chain of evidence that can link the attacker to the incident.[10] Such evidential

---

[7] Barry M. Leiner et. al, "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (October 2009): 22-31, https://doi.org/10.1145/1629607.1629613.

[8] Helen L. Armstrong and Patrick J. Forde, "Internet Anonymity Practices in Computer Crime," *Information Management and Computer Security* 11, no. 5 (2003): 209-215, https://doi.org/10.1108/09685220310500117.

[9] Sanjay Goel, "Anonymity vs. Security: The Right Balance for the Smart Grid," *Communications of the Association for Information Systems* 36, Article 2 (January 2015): 23-32, https://doi.org/10.17705/1CAIS.03602.

[10] Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence," *Communications of the ACM* 54, no. 8 (August 2011): 132-140, DOI: 10.1145/1978542.1978569.

chains may not constitute irrefutable evidence in a court of law. Still, when combined with additional information such as legal, political, intelligence, and policy considerations, the resulting assessment could allow policymakers to formulate a national response to cyberattacks. From a national security perspective, as Healey argued, knowing "who to blame" can be more important than "who did it?"[11] A proper response to this question provides national authorities with the ability to assess the situation during an evolving conflict and weigh possible responses from a range of economic, diplomatic, or other tools at their disposal. As a multi-dimensional issue that draws on all sources of information available, including technical forensics, human and signals intelligence, historical precedents, and geopolitics, attribution of attacks to a state actor in cyber warfare requires a genuinely national effort and the development of corresponding technical and non-technical capabilities. It is through these processes of data collection and sharing, and analysis and cooperation conducted at national and international levels, that digital forensics becomes instrumental in the operationalization and practical evolution of a robust confidence-building measure (CBM) regime.

The tools and techniques of cyberattacks are common to "cyber warfare," "cyber terrorism" and "cyber activism." Only by analyzing the actors, modes of operation, and motivations behind attacks, and their intended or manifested targets, can one differentiate between the three. In contrast to conventional warfare, it is very difficult to distinguish whether attacks on a website or the online theft of data are attributable to individuals in another state who are motivated by financial gain, political or religious ideology, or actions taken by that state's intelligence agency or military (or their proxies). Since states may launch cyberattacks via proxies in other states, attribution difficulties are compounded, and present fundamental challenges during both conflict and peace times, when international cooperation and treaty compliance verification take hold.

Digital forensics involves gathering data logged in different devices, including computers, routers, electronic industrial control systems, and mobile devices,[12,13,14] putting it on the same timeline and making inferences to determine the anatomy of the attack/intrusion. Several pieces of relevant information can be used for tracing the activities of a person or a device, including IP-addresses,

---

[11] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council*, January Issue Brief 2012, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

[12] Rizwan Ahmed and Rajiv V. Dharaskar, "Mobile Forensics: An Overview, Tools, Future Trends and Challenges from Law Enforcement Perspective," in *6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government* (2008), 312-23.

[13] Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, and James Steele, *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data* (Syngress Publishing, 2010).

[14] Michael G. Solomon, K. Rudolph, Ed Tittel, Neil Broom, and Diane Barrett, *Computer Forensics Jumpstart* (Indianapolis, IN: Wiley Publishing Inc., February 2011).

domain names, and time stamps.[15] These individual entries in different log files can be time-correlated to create a chain of evidence and demonstrate activity emanating from a specific source.

An equally important dimension of digital forensics is the detection of intrusion and post-incident analysis, whereby investigators need to understand how an attack was launched, what was stolen, damaged or changed, and how to prevent the attack from occurring in the future.[16] This involves analyzing the internal logs of actors involved in the cyberattack and piecing together evidence from multiple sources into a single timeline of events. The evidence can be collected from hard drives, RAM, USB drives, storage devices, and network appliances. The fundamental problem with such analysis is the sheer volume of the data. Also, to forensically examine data from the past, it needs to be stored. Data storage limitations, especially network devices that generate enormous amounts of data, also limit the possible time frame of analysis.[17] Other useful forensic techniques include analysis of social networks, as well as text analysis from social media to identify cyber warfare activities, such as propaganda, terrorist recruitment, or information exchange. Some of this analysis is done by hand, but a majority of it is done using automated tools that can sift through large volumes of text to flag relevant data for human analysts. Linguistic tools used for text analysis have become much more sophisticated over the last decade, from simple word counting to separating parts of speech and gaining limited language understanding. These forensic tools can help address the problems of attribution and provide means of dealing with contentious issues related to attribution and deflection of responsibility.

Forensics practices are well established and tools are available to rapidly analyze data and draw inferences from it. The data for analyses can be collected from devices and networks within organizations and Internet Service Providers (ISPs). There are, however, fundamental issues with forensic analyses and data collections that cross international borders and reach outside of a nation-state's jurisdictional control. First, much of the data is stored in routers and devices that are with the ISPs, which are subject to local laws. The data can be in multiple sources on the network and needs to be acquired before analysis. If data is not collected shortly after the incident, it can be overwritten. Consequently, administrative delays in coordination across countries can undermine forensics efforts. Additionally, if a state is complicit in the launch of an attack, the veracity of the data itself can be in question. The data could have been doctored, tailored, or completely faked. Second, getting physical access to the perpetrator's computer

[15] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Boston, MA: Academic Press, May 2011).

[16] N.K. McCarthy, *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk* (McGraw-Hill Osborne Media, August 2012).

[17] José Camacho, "Visualizing Big Data with Compressed Score Plots: Approach and Research Challenges," *Chemometrics and Intelligent Laboratory Systems* 135 (July 2014): 110-125, https://doi.org/10.1016/j.chemolab.2014.04.011.

requires a level of cooperation among countries that may be possible in cases of crime, but strained or nonexistent during cyber warfare. Third, all data can be spoofed, i.e., a fake address of origin can be used in packets to conceal the real IP-address, making the problem of identification even more difficult. Finally, the use of anonymizing tools can camouflage the perpetrators further, making attribution complicated.

All of these challenges make technical attribution for international cyber incidents difficult, though not impossible. It is still possible and has dramatically improved over the last few years through sustained intelligence efforts. In addition to data collected directly from ISPs and organizations, data can be collected through the use of honey pots and prepositioned data taps across global networks. Intelligence agencies are continuously monitoring the activities of known actors (including nation states). They are building intelligence dossiers that can be coupled with knowledge gained from digital forensics to make more definitive attributions.

Knowledge of previous events, tools, and techniques of known actors can be used to trace the origins of attacks. There is no automated analysis process; rather, analysts painfully evaluate evidence and make probabilistic judgments for assigning attribution. There are different levels of attribution, with each level becoming more difficult to assign attribution or point of origin (nation-state, hacker group), specific device (computer used to launch an attack), and an individual responsible for launching the attack. It is even harder to accurately pinpoint the sponsor of an attack, in cases where the hacker/group is working as a proxy.

Discussion

There are limits to what digital forensics can accomplish. These tools will only work to the extent that there is a political will for international cooperation in data sharing and analysis. Important first steps would include the establishment of hotlines and the deployment at strategic locations of standard data collection devices that could not be tampered with. These could be foundational to support the forensic analysis of cyberattacks and international determination of instances of cyber warfare. An international body needs to be created and deployed in a neutral country to monitor and evaluate cyber conflicts, with observers present from warring nations. This body would be able to quickly request data access from different sources; lengthy procedures can delay and limit the collection of data, which can be ephemeral. This body will also have the technical expertise to analyze large volumes of data and determine attribution, as well as to confidentially handle intelligence without having to reveal its sources.

Digital forensics practices were developed to effectively piece together the evidence in criminal cases where: the data footprint is small; there is physical access to devices; and the perpetrators involved are relatively inexperienced with camouflaging techniques. This is very rarely the scenario when attacks are perpetrated by well-trained professional hackers. As a result, intelligence agen-

cies have already adapted and scaled forensics procedures for nation-state cyberattacks; a lot of these practices are not yet in the public domain. We will need to create standard forensics procedures (publicly available) for investigating cross border attacks in which camouflaging techniques have been deployed.

Additionally, digital forensics is constantly lagging behind the torrid pace of technological evolution, both in types of applications and devices, as well as in volumes of data.[18] In the coming years, digital forensics will need to be able to contend with the extremely high volumes of data, as well as the sophisticated camouflaging techniques that are used in cyber warfare to become a credible factor in the attribution of cyber warfare activities. To be able to stay on course, we need to have an international forensics research institute for researching and updating forensics practices as information infrastructures evolve (e.g., connected vehicles, human-implantable devices, self-driving cars). We also need to train experts in each country on best practices (tools and techniques) in digital forensics so that they can conduct their investigations.

We must realize that attribution may not always be perfect due to purposeful misdirection or limitations of the analysis itself. This was illustrated by the attack on Sony Pictures Entertainment in November 2014. A hacker group calling itself the "Guardians of Peace" released confidential Sony data onto the Internet, including personal employee data, vast email and password files, internal documents and communications, unreleased copies of motion pictures, and much more. There are two conflicting theories of attribution: one suggests that the North Korean government was behind the attack, given the similarity of the malware used to that used in previous attacks by the North Koreans;[19] the other, based on linguistics analysis, suggests that Russians conducted the attack.[20] There is no conclusive proof supporting either theory, only circumstantial evidence based on the conventional triad of means, motives, and opportunity. To address this, we must resort to a probabilistic approach and define standards of attributions based on the confidence levels of attribution and permissible retaliation to prevent the disproportionate response from escalating into a kinetic conflict.

The demilitarization of cyberspace or a moratorium on the development of cyber weapons is no longer a possibility. However, nation states must come together to find common ground in cyber warfare starting with confidence-building measures, norms of behavior, and the applicability of international laws to reduce the possibility of a major catastrophic incident. Formal information sharing (both at CERT and diplomatic levels) and establishing hotlines will help de-escalate future cyber incidents. There needs to be consensus building at the

---

[18] Simson L. Garfinkel, "Digital Forensics Research: The Next 10 Years," *Digital Investigation* 7, Supplement (August 2010): S64-S73, https://doi.org/10.1016/j.diin.2010.05.009.

[19] Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far," *Wired*, March 12, 2014, https://www.wired.com/2014/12/sony-hack-what-we-know.

[20] Zetter, ''Sony Got Hacked Hard."

United Nations and other established international bodies such as the Office of Security and Cooperation (OSCE) to find ways of building consensus among nation states on preventing cyber conflicts and building confidence.

Conclusions

The Internet is a major economic and societal driver and instrument of knowledge dissemination with huge economic, political, and national security consequences. It is also a place for data theft, espionage, fake news, political influence, and propaganda, as has been evidenced in the Middle East, South Asia, and Europe. Nation-state attacks are constantly growing both in terms of frequency of attacks and sophistication. Such attacks undermine its influence as societal glue and diminish its influence on economic prosperity. There have been efforts to stem the escalation of cyber warfare; however, it has been very hard to build consensus among nation states on the mechanisms for de-escalation of cyber warfare. Lack of transparency in cyber weapon development and attribution of cyberattacks has been a critical barrier to the acceptance of confidence building measures. Improvement in data collection (intelligence) and forensic analytics capabilities has given us a much better cyber incident attribution capability. By building consensus among nation-states on protocols and procedures for attribution and clarifying the applicability of international law, we can start to build consensus on CBMs and norms and make the Internet safer and enable it to thrive. The paper suggests several initiatives to reduce the chances of cyber conflict as well as to prevent cyber conflicts from escalating, such as defining clear processes for attribution, creating neutral bodies for incident analysis, and limiting the scope of retaliation based on the confidence in attribution.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Journal *Connections: The Quarterly Journal*, Vol. 19, 2020 is supported by the United States government.

About the Author

See p. 86 of the current issue, https://doi.org/10.11610/Connections.19.1.07.