Cyber-Attack Attributes

Mehdi Kadivar

> *"The bottom line of security is survival, but it also reasonably includes a substantial range of concerns about the conditions of existence."*
>
> Barry Gordon Buzan
> Professor of International Relations
> Central figure of the Copenhagen School

Cyber-attacks threaten our ability to use the Internet safely, productively, and creatively worldwide and are at the core of many security concerns. The concept of cyber-attacks, however, remains underdeveloped in the academic literature. To advance theory, design and operate databases to support scholarly research, perform empirical observations, and compare different types of cyber-attacks, it is necessary to first clarify the attributes of the "concept of cyber-attack". In this article, attributes of cyber-attacks are identified by examining definitions of cyber-attacks from the literature and information on ten high-profile attacks. Although the article will be of interest to a broad community, it will be of particular interest to senior executives, government contractors, and researchers interested in contributing to the development of an interdisciplinary and global theory of cybersecurity.

Introduction

Senior corporate executives, government officials, and academics have become aware that there are: i) serious financial and regulatory costs arising from cyber-attacks (Pearson, 2014; Sugarman, 2014; US Securities and Exchange Commission, 2014); ii) vulnerabilities in high-value assets such as supervisory-control and data-acquisition systems (Ashford, 2013; Crawford, 2014; Kovacs, 2014; Nicholson et al., 2012; Weiss, 2014); iii) concerns about the upcoming deployment of the "Internet of Things" (IoT) (NSTAC, 2014); and iv) few constraining mechanisms to inhibit malicious behaviours of threat actors (Castel, 2012; Jowitt, 2014, Scully, 2013; Sugarman, 2014; Weiss, 2014).

The urgency of research and development is underlined by the US National Security Telecommunications Security Advisory Committee (NSTAC, 2014): "There is a small – and rapidly closing – window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations." This state-of-affairs has parallels to the experience with supervisory control and data acquisition systems, though in that case the threat space evolved over time. With the Internet of Things, the NSTAC believes that the window of time in which we can take action will only be open for another three to five years.

Although the word "cyber-attack" is used frequently, its meaning remains obscure (Hathaway et al., 2012, Roscini, 2014). In this article, the approach to clarify what is meant by cyber-attack is similar to the approach researchers followed to clarify what was meant by "security" in the late 1990s (e.g., Baldwin, 1997; Buzan, 1998; Huysmans, 1998). Security researchers identified essential attributes to make explicit what was meant by security. They eliminated ambiguities and inconsistencies in the different uses of the security concept. Their objective was not to produce another one-sentence definition of security; they set out to identify the essential attributes of security.

This article contributes a set of attributes of the cyber-attack concept. It does so by examining various definitions published in the literature and information on ten high-profile cyber-attacks. The main motivation for identifying the attributes of cyber-attacks is to enable building the theory of cyber-attacks as a unity of intellectual frameworks beyond the disciplinary perspectives (i.e., a transdisciplinary theory).

Cyber-Attack Attributes

Mehdi Kadivar

The remainder of this article infers the essential attributes of the cyber-attack concept from definitions of cyber-attacks found in the literature, synthesizes information on ten high-profile cyber-attacks, and uses it to provide concrete examples of the attributes of cyber-attacks.

Attributes from Definitions of Cyber-Attacks

The journal articles published in the English language by organizations in North America and Europe were reviewed for the purpose of identifying definitions of "cyber-attack". The following six definitions of cyber-attack were identified:

1. "Any action taken to undermine the functions of a computer network for a political or national security purpose." (Hathaway et al., 2012: p. 821)

2. "Use of deliberate actions – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks." (Owens et al., 2009: p. 10)

3. "Operations, whether in offence or defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer system or network." (Roscini, 2014: p. 17)

4. "An exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money." (Uma & Padmavathi, 2013: p. 390)

5. "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. " (US Joint Chiefs of Staff, 2010: p.5).

6. "Efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them." (Waxman, 2011: p. 422)

Each definition shown above addresses one or more of the following five questions: i) What types of assets do cyber-attacks target?; ii) What effect do cyber-attacks have on assets targeted?; iii) What motivates cyber-attacks?; iv) Which actors are involved in cyber-attacks?; and v) What are the durations of cyber-attacks?

The six definitions identified suggest that the concept of cybersecurity has at least five attributes.

1. *Actors:* At least two actors are involved in each cyber-attack: the owner of the asset that is targeted and an adversary (US Joint Chiefs of Staff, 2010). The definitions of cyber-attack are not concerned with the nature of the adversaries. The offensive and defensive operations can be carried out by nation states, companies, groups, collectives, or individuals.

2. *Assets targeted:* Five of the six definitions provided above identify the assets cyber-attacks target. These assets include: computer systems and networks (Hathaway et al., 2012; Owens et al., 2009; US Joint Chiefs of Staff, 2010; Waxman, 2011); information, programs, or functions resident in or transiting systems or networks (Hathaway et al., 2012; Owens et al., 2009, Roscini, 2014; Waxman, 2011); computer-operated physical infrastructure (Roscini, 2014); and physical objects extrinsic to a computer, computer system, or network (Roscini, 2014).

3. *Motivation:* The motivations for cyber-attacks include accessing unauthorized or secure information, spying, and stealing both data and money (Uma & Padmavathi, 2013); national security and political causes (Hathaway et al., 2012); and propaganda or deception (Roscini, 2014).

4. *Effect on targeted assets:* Cyber-attacks result in the alteration, deletion, corruption, deception, degradation, disablement, disruption, or destruction of assets (Owens, et al., 2009; Roscini, 2014; Uma & Padmavathi, 2013; Waxman, 2011) as well as denying access to assets (Roscini, 2014). Definitions of cyber-attacks identify logical, physical, and cognitive effects on assets. Denial of access to assets is an example of logical effects. Cognitive effects include deception, meaning the use of false information to convince an adversary that something is true. Destruction of capital assets is an example of physical effects.

5. *Duration:* Only one definition of cyber-attacks mentions its intended duration. The definition by Owens, Dam, and Lin (2009) includes the possibility of a cyber-attack over an extended duration.

Cyber-Attack Attributes

Mehdi Kadivar

Examination of High-Profile Cyber-Attacks

Information on 10 high-profile cyber-attacks was examined for the purpose of i) collecting data for the five attributes identified from the definitions of cyber-attacks and ii) identifying additional attributes. A security expert who provided advice throughout this research helped select the 10 high-profile cyber-attacks that would result in the highest possible diversity of industries in which the target organizations operated. He also helped identify reliable online sources of information about these cyber-attacks.

The use of high-profile attacks was purposeful. The intent was to gather as much information as possible about an attack from reliable sources. Upfront, it was clear that the selection of high-profile cyber-attacks would prevent overgeneralizing findings to attacks that were not high profile.

For each high-profile cyber-attack, a scenario was developed. A cyber-attack scenario is a description of the sequence of events that results from the interactions among the individuals and organizations involved in a cybersecurity breach as well as their stakeholders. A cybersecurity breach refers to an event where an individual has obtained information on a protected computer that the individual lacks authorization to obtain by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information. The main actors in a cyber-attack scenario are the “known target” and the “alleged attacker.”

Attributes of High-Profile Cyber-Attacks

For each of the 10 cyber-attacks examined, Table 1 provides the information collected for the five attributes identified from the examination of the definitions of cyber-attacks.

Eight of the 10 cyber-attacks shown in Table 1 meet Damballa’s (2010) definition of an advanced persistent threat: a cyber-attack that requires a high degree of stealthiness over a prolonged duration of operation in order to be successful. The two cyber-attacks in Table 1 that are not advanced persistent threats are (5) CyberBunker’s distributed denial-of-service attack on The Spamhaus Project and (9) Criminals who encrypt and decrypt data in users’ computers. An advanced persistent threat attack is sophisticated and seeks to achieve ongoing access without discovery (Hashimoto et al., 2013). The duration of the advanced persistent threats ranged from 8 to 32 weeks. Four of the advanced persistent threats contained customized code specifically developed for the attack: the attacks that targeted (1) Google, (2) Iran, (6) Target Corporation, and (7) TJX Companies.

The examination of these 10 cyber-attacks suggested that at least six additional cyber-attack attributes exist:

1. *Attack vector:* The path or means by which an attacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. An attack vector enables the exploitation of system vulnerabilities. Seven of the 10 cyber-attacks examined started with phishing or spear phishing (i.e., an email that appears to be from an individual or business that the user knows, but it is not). The cyber-attacks that started with phishing include those that targeted: (6) Target Corporation, (8) Bank customers, and (9) Computer owners. Those that started with spear phishing include: (1) Google, (3) New York Times, (4) Chemical and defence firms in United States, and (10) Gaming companies.

2. *Vulnerability:* Any form of weakness in a computing system or environment that can let attackers compromise a system's or environment’s confidentiality, integrity, and availability (Foreman, 2009). A vulnerability is a weakness or gap in the efforts to protect an asset. A total of 18 vulnerabilities were exploited in the 10 cyber-attacks examined, and they can be organized into the five types specified in the United Kingdom’s implementation of "ISO/IEC 27005: 2008: Hardware, Software, Network, Site and Personnel/Users (ISO, 2008). In our small sample, people and software account for 14 of the 18 vulnerabilities that attackers exploited.

3. *Malicious software:* Refers to software programs designed to damage or do other unwanted actions on a computer system. A variety of malicious software programs were used in the cyber-attacks examined. They include: Hydraq, Stuxnet, Poison Ivy, Botnet malware, Citadel, BlackPOS, Blabla sniffing, SpyEye, Nitro, and PlugX.

4. *Botnet reliance:* Refers to the cyber-attacks dependence on botnets (i.e., networks of computers infected with malicious software and controlled as a group without the owners' knowledge). Eight cyber-attacks relied on botnets: (1) Google, (3) New York Times, (4)

Cyber-Attack Attributes

Mehdi Kadivar

Table 1. Five attributes of high-profile cyber-attacks

Attack	1. Actor: Known Target	1. Actor: Alleged Attacker	2. Asset Targeted	3. Motivation	4. Effect on Targeted Asset	5. Attack Duration
1	Google (multinational specializing in Internet-related services and products)	Elderwood Gang (large Chinese cyberespionage organization)	Source code repositories that support supply chain functions	Collect valuable proprietary information of businesses	Gmail database was modified to allow extraction of information without detection	28 weeks (Jun to Dec '09)
2	Iran	Israel & US	Nuclear centrifuges controlled by computers at Natanz, Iran	Delay Iran's nuclear R&D program	1,000 centrifuges destroyed	32 weeks (Nov '07 to Jun '10)
3	New York Times: publisher of American daily newspaper	Hackers who used methods of the Chinese military	Passwords and data of reporters and other employees	Obtain names of people who provided information about relatives of China's prime minister accumulating billions through business dealings	Data of 50 employees copied and uploaded to external server without detection	28 weeks (Oct '12 to Jan '13)
4	Chemical & defence firms in US	Covert Grove (group located in Hebei region in China)	Domain administrator credentials and networks of computers that store information	Collect valuable proprietary information of businesses	Data from 48 companies copied and uploaded to external server without detection	12 weeks (Jul to Sep '11)
5	The Spamhaus Project (not-for-profit that tracks spammers)	CyberBunker (an Internet service provider)	The Spamhaus Project website	Retaliate against Spamhaus for identifying CyberBunker as hosting spammers and asking its upstream service provider to cancel service	Website not available to users	2 weeks (Mar '13)
6	Target Corporation (American discount retailer)	Criminal group	Confidential customer information	Obtain confidential information	Data from 110 million customers copied and uploaded to external server without detected	8 weeks (Nov to Dec '13)
7	TJX Companies (American apparel and home goods company)	Criminal group	Credit and debit card numbers	Obtain confidential information to sell	Data from 94 million customers copied and uploaded to external server without detection	32 weeks (May '06 to Jan '07)
8	Bank customers	Aleksandr Andreevich Panin, a.k.a. "Gribodemon" and "Harderman" (Hacker)	1.4 million computers that store online banking credentials, credit card data, user names, PINs, and other sensitive information	Obtain confidential information to sell	Sensitive information in 30,000 bank accounts was copied and uploaded to external server without detection	In progress
9	Computer owners	Criminals	Users' data or systems	Demand ransom to restore access	250,000 computers encrypted	In progress
10	Gaming companies	Criminals	Digital certificates for the secure exchange of information over the Internet using the public key infrastructure	Obtain confidential information to sell	Data from up to 30 gaming companies copied and uploaded to external server without detection	In progress

Cyber-Attack Attributes

Mehdi Kadivar

Chemical and defence firms, (5) The Spamhaus Project, (6) Target Corporation, (8) Bank customers, (9) Computer owners, and (10) Gaming companies.

5. *Origin:* Refers to the geographical origin of the cyber-attack. Four of the 10 cyber-attacks in the sample were alleged to have originated from China: (1) Google, (3) New York Times, (4) Chemical and defence firms, and (10) Gaming companies; four were from Eastern Europe (6) Target Corporation, (7) TJX Companies, (8) Bank customers, and (9) Computer owners: one originated from the United Kingdom and Spain; and one was from Israel and the United States.

6. *Destination:* Refers to the region affected by the cyber-attack in the near term. Eight of the 10 high-profile cyber-attacks targeted organizations in the United States. The two cyber-attacks that did not target organizations in the United States were (2) Iran and (5) The Spamhaus Project. However, seven of the eight attacks that targeted organizations in the United States also targeted organizations in other parts of the world (i.e., Australia, Bahrain, Bangladesh, Brazil, Canada, China, Eastern Europe, France, India, Ireland, Mexico, Oman, Puerto Rico, Russia, Saudi Arabia, South East Asia, and the United Kingdom).

Conclusion

Through the analysis of six definitions of the term cyber-attack and ten high-profile cases of cyber-attack, this article identified 11 important attributes of cyber-attacks following an approach similar to the one that was used in the late 1990s to clarify what is meant by "security". In summary, these attributes are:

1. Actors
2. Assets targeted
3. Motivation
4. Effect on targeted assets
5. Duration
6. Attack vector
7. Vulnerability
8. Malicious software
9. Botnet reliance
10. Origin
11. Destination

These attributes could be further categorized as Attack Intent (Actors, Origin, Destination, Motivation), Attack Impact (Assets targeted, Effect on targeted assets, Duration) and Attack Path (Initiation approach, Vulnerability, Malicious software, Botnet reliance).

Cyber-attack studies are at the core of cybersecurity studies. However, what is meant by "cyber-attack" is not clear and the field is underdeveloped. Definitions of cyberattack vary (Hathaway et al., 2012; Owens et al., 2009), and some are ambiguous. Ambiguous definitions of cyber-attacks hamper the prosecution of criminals (Whitehouse, 2014).

The analysis carried out opens up interesting areas for future research. For example, this study examined 10 instances of *successful* cyber-attacks; future studies can examine the attributes of cyber-attacks that failed or were only partially successful. The purpose of studying failed cyber-attacks or those that were partially successful is to identify missteps, symptoms, causes, and the reasons that attackers came and went.

About the Author

Mehdi Kadivar is completing his MASc in Technology Innovation Management at Carleton University in Ottawa, Canada. He holds a Bachelor of Science degree in Business Administration from the American University of Sharjah, Iran. Previously, he worked as a system maintenance expert at the Petrochemical Industries Design and Engineering company and as an intern at the Emirates National Bank of Dubai.

References

Ashford, W. 2013. US Researchers Find 25 Security Vulnerabilities in SCADA Systems. *ComputerWeekly.com*, October 18. http://www.computerweekly.com/news/2240207488/US-researchers-find-25-security-vulnerabilities-in-SCADA-systems

Blank, L.R. 2013. International Law and Cyber Threats from Non-Sate Actors, *International Law Studies,* 89:157-197. http://ssrn.com/abstract=2194180

Buzan, B. 1991. *People, States and Fear: An Agenda for Security Analysis in the Post-Cold War Era.* Brighton: Wheatsheaf.

Buzan, B., Waever, O., & De Wilde, J. 1998. *Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner Publishers.

Castel, M. E. 2012. International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors. *Canadian Journal of Law & Technology,* 10(1): 89-120. https://ojs.library.dal.ca/CJLT/article/view/4833/4353

Cyber-Attack Attributes

Mehdi Kadivar

Crawford, J. 2014. The U.S. Government Thinks China Could Take Down the Power Grid. *CNN*, November 20. http://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/

Damballa. 2010. Advanced Persistent Threats: A Brief Description. *Damballa, Inc.* Accessed November 1, 2014: http://www.damballa.com/advanced-persistent-threats-a-brief-description/

Foreman, P. 2009. *Vulnerability Management.* Boca Raton, FL: Auerbach Publications.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. 2012. The Law of Cyber-Attack. *California Law Review*. 100(4): 817-885. http://www.californialawreview.org/articles/the-law-of-cyber-attack

Huysmans, J. 1998. Security! What Do You Mean? From Concept to Thick Signifier. *European Journal of International Relations,* 4(2): 226-255. http://dx.doi.org/10.1177/1354066198004002004

ISO. 2008. ISO/IEC 27005:2008: Information Technology - Security Techniques - Information Security Risk Management. *International Organization for Standardization.* Accessed November 1, 2014: http://www.iso.org/iso/catalogue_detail?csnumber=42107

Jowitt, T. 2014. White House Advisory Group: Governments Have Five Years To Secure IoT. *TechWeek Europe*, November 20. http://www.techweekeurope.co.uk/e-regulation/governments-secure-iot-156149

Kaspersky Lab. 2014. Malware Classifications. *Kaspersky Lab.* Accessed November 1, 2014: http://www.kaspersky.com/internet-security-center/threats/malware-classifications

Kovacs, E. 2014. U.K. Invests Heavily in ICS Cyber Security Research. *Security Week,* October 3. http://www.securityweek.com/uk-invests-heavily-ics-cyber-security-research

National Security Telecommunications Security Advisory Committee. 2014. *Draft Report to the President on the Internet of Things,* November. Washington, DC: Department of Homeland Security.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. 2012. SCADA Security in the Light of Cyber-Warfare. *Computers & Security,* 31(4):418-436. http://dx.doi.org/10.1016/j.cose.2012.02.009

O'Connell, M.E. 2012. Cyber Security without Cyber War. *Journal of Conflict and Security Law,* 17(2): 187-209. http://dx.doi.org/10.1093/jcsl/krs017

Owens, W. A., Dam, K., & Lin, H. S. 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities*. Washington, DC: National Academies Press.

Pearson, N. 2014. A Larger Problem: Financial and Reputational Risks. *Computer Fraud & Security,* 2014(4): 11-13. http://dx.doi.org/10.1016/S1361-3723(14)70480-4

Rattray, G., & Healey, J. 2010. *Categorizing and Understanding Offensive Cyber Capabilities and Their Use. Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: National Academies Press.

Roscini, M. 2014. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Scully, T. 2013. The Cyber Security Threat Stops in the Boardroom. *Journal of Business Continuity & Emergency Planning,* 7(2):139-147. http://www.ncbi.nlm.nih.gov/pubmed/24457325

Sugarman, E. 2014. Cybersecurity is a Severe and Growing Challenge for Government Contractors. *Forbes*, August 24. http://www.forbes.com/sites/elisugarman/2014/08/26/cybersecurity-is-a-severe-and-growing-challenge-for-government-contractors/

Šulović, V. 2010. *Meaning of Security and the Theory of Securitization.* Belgrade: Belgrade Center of Security Policy.

Uma, M., & Padmavathi, G. 2013. A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security,* 15(5): 390-396.

US Securities and Exchange Commission. 2014. Form 8-K (001-15935): Community Health Systems, Inc. *United States Securities and Exchange Commission,* August 18. http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm

United States Joint Chiefs of Staff. 2010. Memorandum: Joint Terminology for Cyberspace Operations. Washington, DC: United States Department of Defense.

Weiss, M. 2014. Do We Need a CDC for Cybersecurity? *CIO Insight,* October 30. http://www.cioinsight.com/security/do-we-need-a-cdc-for-cybersecurity.html

Whitehouse, S. 2014. Opening Statement: Judiciary Subcommittee on Crime and Terrorism Hearing on Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks, July 15. Washington, DC: U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism. http://www.hsdl.org/?view&did=756247

Citation: Kadivar, M. 2014. Cyber-Attack Attributes. *Technology Innovation Management Review*, 4(11): 22–27. http://timreview.ca/article/846

Keywords: cyber-attack, attributes, cybersecurity, attack characteristics