Defining Cybersecurity

Article · October 2014

CITATIONS
5

READS
15,470

1 author:

Nadia Diakun-Thibault
North Carolina State University
5 PUBLICATIONS **68** CITATIONS

SEE PROFILE

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

> *"To choose a definition is to plead a cause."*
>
> Charles Leslie Stevenson (1908–1979)
> Analytic philosopher

Cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. In conjunction with an in-depth literature review, we led multiple discussions on cybersecurity with a diverse group of practitioners, academics, and graduate students to examine multiple perspectives of what should be included in a definition of cybersecurity. In this article, we propose a resulting new definition: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to cybersecurity challenges.

Introduction

The term "cybersecurity" has been the subject of academic and popular literature that has largely viewed the topic from a particular perspective. Based on the literature review described in this article, we found that the term is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative. There is a paucity of literature on what the term actually means and how it is situated within various contexts. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. For example, there is a spectrum of technical solutions that support cybersecurity. However, these solutions alone do not solve the problem; there are numerous examples and considerable scholarly work that demonstrate the challenges related to organizational, economic, social, political, and other human dimensions that are inextricably tied to cybersecurity efforts (e.g., Goodall et al., 2009; Buckland et al., 2010; Deibert, 2012). Fredrick Chang (2012), former Director of Research at the National Security Agency in the United States discusses the interdisciplinary nature of cybersecurity:

"A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed."

In attempting to arrive at a more broadly acceptable definition aligned with the true interdisciplinary nature of cybersecurity, we reviewed relevant literature to identify the range of definitions, to discern dominant themes, and to distinguish aspects of cybersecurity. This research was augmented by multiple engagements with a multidisciplinary group of cybersecurity practi-

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

tioners, academics, and graduate students. Together, these two activities resulted in a new, more inclusive, and unifying definition of cybersecurity that will hopefully enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby influence the approaches of academia, industry, and government and non-government organizations to cybersecurity challenges. This article reflects the process used to develop a more holistic definition that better situates cybersecurity as an interdisciplinary activity, consciously stepping back from the predominant technical view by integrating multiple perspectives.

Literature Review

Our literature review spanned a wide scope of sources, including a broad range of academic disciplines including: computer science, engineering, political studies, psychology, security studies, management, education, and sociology. The most common disciplines covered in our literature review are engineering, technology, computer science, and security and defence. But, to a much lesser extent, there was also evidence of the topic of cybersecurity in journals related to policy development, law, healthcare, public administration, accounting, management, sociology, psychology, and education.

Cavelty (2010) notes there are multiple interlocking discourses around the field of cybersecurity. Deconstructing the term cybersecurity helps to situate the discussion within both domains of "cyber" and "security" and reveals some of the legacy issues. “Cyber” is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality (Oxford, 2014). It evolved from the term "cybernetics", which referred to the “field of control and communication theory, whether in machine or in the animal” (Wiener, 1948). The term "cyberspace" was popularized by William Gibson’s 1984 novel, *Neuromancer*, in which he describes his vision of a three-dimensional space of pure information, moving between computer and computer clusters where people are generators and users of the information (Kizza, 2011). What we now know as cyberspace was intended and designed as an information environment (Singer & Friedman, 2013), and there is an expanded appreciation of cyberspace today. For example, Public Safety Canada (2010) defines cyberspace as “the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where… people are linked together to exchange ideas, services and friendship.” Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors (Deibert & Rohozinski, 2010), who represent the range of human intentions.

As for the term "security", in the literature we reviewed, there appeared to be no broadly accepted concept, and the term has been notoriously hard to define in the general sense (Friedman & West, 2010; Cavelty, 2008). According to Buzan, Wæver, and Wilde (1998), discourses in security necessarily include and seek to understand who securitizes, on what issues (threats), for whom (the referent object), why, with what results, and under what conditions (the structure). Although there are more concrete forms of security (e.g., the physical properties, human properties, information system properties, or mathematical definitions for various kinds of security), the term takes on meaning based on one’s perspective and what one values. It remains a contested term, but a central tenet of security is being free from danger or threat (Oxford, 2014). Further, although we have indicated that security is a contested topic, Baldwin (1997) states that one cannot use this designation as “an excuse for not formulating one’s own conception of security as clearly and precisely as possible”.

As a result of our literature review, we selected nine definitions of cybersecurity that we felt provided the material perspectives of cybersecurity:

1. “Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders.” (Kemmerer, 2003)

2. “Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.” (Lewis, 2006)

3. “Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on.” (Amoroso, 2006)

4. “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.” (ITU, 2009)

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

5. "The ability to protect or defend the use of cyberspace from cyber-attacks." (CNSS, 2010)

6. "The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability." (Public Safety Canada, 2014)

7. "The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure." (Canongia & Mandarino, 2014)

8. "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014)

9. "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (DHS, 2014)

Although some of these definitions include references to non-technical activities and human interactions, they demonstrate the predominance of the technical perspective within the literature. As stated by Cavelty (2010), the discourse and research in cybersecurity "necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat". Accordingly, within their particular context, the definitions above are helpful but do not necessarily provide a holistic view that supports interdisciplinarity. Referring back to Buzan, Wæver, and Wilde's (1998) discussion of securitization studies, any definition should be able to capture an understanding of the actor, subject, the referent object, the intentions and purposes, the outcomes, and structure. In our review of the literature, we did not find a definition that is inclusive, impactful, and unifying. Cybersecurity is a complex challenge requiring interdisciplinary reasoning; hence, any resulting definition must attract currently disparate cybersecurity stakeholders, while being unbiased, meaningful, and fundamentally useful.

Towards a New Definition

Faced with many definitions of cybersecurity from the literature, we opted for a pragmatic qualitative research approach to support the definitional process, which melds objective qualitative research with subjective qualitative research (Cooper, 2013). In effect, the result is a notional definition that is grounded in objectivity (e.g., an intrusion-detection system) versus supposition (e.g., the intentions of a hacker). This definitional process included: a review of the literature, the identification of dominant themes and distinguishing aspects, and the development of a working definition. This definition was in turn introduced to the multidisciplinary group discussions for further exploration, expansion, and refinement to arrive at the posited definition.

Dominant themes

In our literature review, we identified five dominant themes of cybersecurity: i) technological solutions; ii) events; iii) strategies, processes, and methods; iv) human engagement; and v) referent objects (of security). Not only do these themes support the interdisciplinary nature of cybersecurity, but, in our view, help to provide critical context to the definitional process.

Distinguishing aspects

In conjunction with the emergence of the themes, we formulated distinguishing aspects of cybersecurity, initially through discussion amongst the authors to be refined later through the multidisciplinary group discussions. In the end, we identified that cybersecurity is distinguished by:

- its interdisciplinary socio-technical character
- being a scale-free network, in which the capabilities of network actors are potentially broadly similar
- high degrees of change, connectedness, and speed of interaction

Through the process, there was consensus within the multidisciplinary group to adopt the view that the Internet is a scale-free network (e.g., Barabási & Albert, 1999), meaning it is a network whose degree distribution follows a power law, at least asymptotically. Even though this characterization of the Internet is a subject of debate (e.g., Wallinger et al., 2009), we argue that there are cyber-attack scenarios, and especially the evolution of malware markets, where the capabilities

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

for launching attacks has been largely commoditized, hence flattening the space of network actors.

Throughout the initial part of the process that resulted in a working paper, we intentionally attempted to redress the technical bias of extant definitions in the cybersecurity literature by ensuring that scholars and practitioners contributed to the discussion and were provided an opportunity to review and comment on our initial definition, themes, and distinguishing aspects. To expand the discussion and create additional scholarly dialogue, we posited an original "seed" definition for discussion and further refinement during two three-hour engagements with a multidisciplinary group of cybersecurity practitioners, academics, industry experts from the VENUS Cybersecurity Institute (venus cyber.com), and graduate students in the Technology Innovation Management program (timprogram.ca) at Carleton University in Ottawa, Canada.

Emergent definitions of cybersecurity

Our engagement with the multidisciplinary group primarily consisted of providing selected readings from the literature, an initial presentation and discussion of our own work to date, followed by a syndicate activity related to distinguishing aspects and defining cybersecurity. Three syndicates were formed from the group and they were asked to develop their own definitions. These definitions, along with the authors' brief critiques, are presented in Table 1. The first two definitions were developed by the authors, whereas the next three definitions arose from group participants.

Table 1. Emergent cybersecurity definitions and critiques

	Participant Working Definitions	Critique(s)
1	"Cybersecurity is the protection of information/data, assets, services, and systems of value to reduce the probability of loss, damage/corruption, compromise, or misuse to a level commensurate with the value assigned."	In the main, the feedback suggested that the inclusion of value introduced the human concepts related to security, but that the definition was too prescriptive and suffered the problem of a restrictive "listing" of what is being protected.
2	"Cybersecurity is a collection of interacting processes intended to protect cyberspace and cyberspace-enabled systems (collectively resources) from intentional actions designed to misalign actual resource property rights from the resource owner perceived property rights."	This definition introduced the emerging cyber-physical environment and included the important concept of control over property rights. However, the definition's focus on "human intentional actions" was viewed as being overly restrictive.
3	"Cybersecurity is a collection of interacting processes intended to make cyberspace safe and secure."	Specifically intended to be broader than the seed definition, this definition introduced more problems than it solved because it was unnecessarily broad and introduced the contested notion of safety with security.
4	"Cybersecurity is a domain dedicated to the study and practice of the protection of systems or digital assets from any action taken to impose authorization on those systems or digital assets that do not align with the property rights of the resource facility as understood by its owner."	In this definition, the concepts of property rights and control were introduced. However, there were concerns about the potential implications of "action taken" to mean limiting cybersecurity to human actors. Also there were concerns regarding the terms, which imposed limits on the scope of the definition such as "study" and "practice", thereby situating the issues largely within the academic domain.
5	"Cybersecurity is the state in which power over the execution of computers (sensu lato) and over information in the control of computers is where it should be."	This definition reinforced the notions of control over information and systems. The main criticism was defining cybersecurity as a state.

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

A New Definition of Cybersecurity

We propose the following definition, which integrates key concepts drawn from the literature and engagement with the multidisciplinary group:

Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure *from* de facto *property rights.*

We deconstruct this definition as follows:

- *…the organization and collection of resources, processes, and structures…*: This aspect captures the multiple, interwoven dimensions and inherent complexity of cybersecurity, which ostensibly involve interactions between humans, between systems, and between humans and systems. By avoiding discussion of which resources, processes, or structures, the definition becomes non-prescriptive and recognizes the dynamic nature of cybersecurity.

- *…used to protect cyberspace and cyberspace-enabled systems…*: This aspect includes protection, in the broadest sense, from all threats, including intentional, accidental, and natural hazards. This aspect also incorporates the traditional view of cyberspace but includes those systems that are not traditionally viewed as part of cyberspace, such as computer control systems and cyber-physical systems. By extension, the protection applies to assets and information of concern within cyberspace and connected systems.

- *…from occurrences…*: This aspect recognizes that "protections" are intended to address the full range of intentional events, accidental events, and natural hazards. It also suggests that some of the occurrences are unpredictable.

- *…that misalign* de jure *from* de facto *property rights…*: This aspect incorporates the two separate notions of ownership and control that dominate discussion of cybersecurity and digital assets introduced in the property rights framework of Ostrom and Hess (2007), which include access, extraction, contribution, removal, management, exclusion, and alienation. Any event or activity that misaligns actual (*de facto*) property rights from perceived (*de jure*) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident.

Substantiating Our Definition

As discussed earlier, our definition should engender greater interdisciplinary and collaborative efforts on cybersecurity. Our goal is to "bring together" not to "push apart" or "isolate". Our success (or failure) can be partly validated if we can demonstrate that:

1. We can map other definitions of cybersecurity into our definition.

2. Our definition is unifying and inclusive in that it supports interdisciplinarity.

To assist in the analysis and mapping of the definitions to our new definition, we identified conceptual categories from definitions drawn from the literature as well as our own definition (Table 2). Unless otherwise cited, the category definitions are drawn largely from the Oxford (2014) online dictionary. The exact wordings of the definitions are meant to be as encompassing as possible.

A number of definitions of cybersecurity were presented in this article. Some of the definitions are from the literature and drive the perspectives of certain communities. Other definitions arose through our group discussions and related activities. Table 3 provides examples of how our analysis was applied to sample definitions from the literature and group discussions.

The above analysis helps to demonstrate that our new definition is inclusive of key components from a sample of extant and participant definitions. Furthermore, three of the dominant themes – technological solutions; strategies, processes, and methods; and human engagement – are all refinements of the "the organization and collection of resources, processes, and structures used to protect..." component of our definition. The dominant theme of "events" is a refinement of "occurrences." We also view "referent objects (of security)" as a refinement of "cyberspace and cyberspace-enabled systems." Retrospectively, we therefore show how our definition is consistent with the dominant themes of cybersecurity and reflects the previously identified distinguishing aspects. Therefore, this mapping illustrates how our definition supports interdisciplinarity.

Conclusion

We have provided a new, more inclusive, and unifying definition of cybersecurity that we believe will enable an enhanced and enriched focus on interdisciplinary cy-

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

bersecurity dialectics and, thereby, will influence the approaches of researchers, funding agencies, and organizations to cybersecurity challenges. For example, the new definition and associated perspectives could lead to changes in public policy and inform legislative actions.

The definition resulting from the work reported herein has a number of potentially salutary features, including:

1. Contributing a major unifying theme by positioning cybersecurity as an interdisciplinary domain, not a technical domain.

2. Supporting inclusiveness demonstrated through the relationship to the five dominant cybersecurity themes and mapping to previous definitions.

3. Incorporating the evolution towards a more interconnected world through inclusion of both cyberspace and cyberspace-enabled systems. The latter includes cyber-physical systems and control systems.

4. Using protection – as a fundamental concept within security – in a broad sense within the definition, including protection from intentional events, accidental events, and natural hazards.

5. Incorporating the "property rights" framework of Ostrom and Hess (2007), which includes access, extraction, contribution, removal, management, exclusion, and alienation. Thus, the discussion moves beyond traditional assets and information terms to broadly include that which has meaning or value.

The absence of a concise, universally acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges. It has become increasingly apparent that cybersecurity is interdisciplinary. The more inclusive, unifying definition presented in this article aims to facilitate interdisciplinary approaches to cybersecurity. We hope that the definition will be embraced by the multiple disciplines engaged in cybersecurity efforts, thereby opening the door to greater understanding and collaboration needed to address the growing and complex threats to cyberspace and cyberspace-enabled systems.

Table 2. Conceptual categories and their definitions

Category	Definition
Asset	In general, defined as "a useful or valuable thing or person". Here, we refine the definition to refer to "cyberspace and cyberspace-enabled systems".
Capability	An abbreviation for the organization and combination of resources, processes, and structures.
Misalign	Align is defined as "put (things) into correct appropriate relative positions"; hence, misalign results in incorrect or inappropriate positions.
Occurrence	An incident or event.
Organization	"A firm's policies and procedures 'organized to exploit the full competitive potential of its resources and capabilities'" (Kozlenkova et al., 2013). We generalize "firms" to "institutions".
Process	The fact of going on or being carried on, as a action or series of actions; progress, course. *in (the) process of (doing something):* in the course of; in the act of carrying out (a particular task, etc.). *in process:* going on, being done; in progress
Property right	An enforceable authority to undertake particular actions in specific domains. Includes the rights of access, withdrawal, management, exclusion, and alienation (Ostrom & Hess, 2007).
Protect	Keep safe from harm or injury.
Resource	"Tangible and intangible assets ['firms'] use to conceive of and implement [their] strategies" (Kozlenkova et al., 2013). We generalize "firms" to "institutions".

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

Table 3. Examples of cybersecurity definitions and related analysis of the proposed definition

Definitions of Cybersecurity	**Analysis** (Key Terms → Corresponding Terms in Proposed Definition)
"The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014)	"protected" → PROTECT "criminal or unauthorized use" → MISALIGN "electronic data" → ASSETS and PROPERTY RIGHTS "measures taken..."→ CAPABILITY
"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." (DHS, 2014)	"activity or process, ability or capability, or state" → CAPABILITY " information and communications systems and the information contained therein" → ASSETS and PROPERTY RIGHTS "protected from and/or defended" → PROTECT "damage, unauthorized use or modification, or exploitation" → MISALIGN
"Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption." (Lewis, 2006)	"safeguarding" → CAPABILITY "computer networks and information" → ASSETS and PROPERTY RIGHTS "penetration and from malicious damage or disruption" → OCCURRENCES or MISALIGN
"Cybersecurity involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on." (Amoroso, 2006).	"involves reducing the risk" → CAPABILITY "of malicious attack" → OCCURRENCES or MISALIGN "software, computers and networks" → ASSETS and PROPERTY RIGHTS "includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on" → CAPABILITY
"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." (ITU, 2009)	"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies" → CAPABILITY "to protect" → PROTECT "cyber environment and organization and user's assets" → ASSETS and PROPERTY RIGHTS
"Cybersecurity is a collection of interacting processes intended to make cyberspace safe and secure." (Definition from group discussions)	"interacting processes" → PROCESS and CAPABILITY "safe and secure" → PROTECT
"Cybersecurity is the state in which power over the execution of computers (sensu lato) and over information in the control of computers is where it should be." (Definition from group discussions)	"power over the execution of computers and over information in the controls of computers is where it should be"→ ASSETS and PROPERTY RIGHTS

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

About the Authors

Dan Craigen is a Science Advisor at the Communications Security Establishment in Canada. Previously, he was President of ORA Canada, a company that focused on High Assurance/Formal Methods and distributed its technology to over 60 countries. His research interests include formal methods, the science of cybersecurity, and technology transfer. He was the chair of two NATO research task groups pertaining to validation, verification, and certification of embedded systems and high-assurance technologies. He received his BScH and MSc degrees in Mathematics from Carleton University in Ottawa, Canada.

Nadia Diakun-Thibault is Senior Science and Analytics Advisor at the Communications Security Establishment in Canada. She holds a Master's degree in Public Administration from Queen's University in Kingston, Canada, and an ABD (PhD) degree in Slavic Languages and Literatures from the University of Toronto, Canada. She has served as Parliamentary Advisor to Members of Parliament and held an Order-in-Council appointment to the Province of Ontario's Advocacy Commission. Her research interests include neurophilosophy, semiotics, linguistics, and public policy. She is also an adjunct faculty member in the Department of Computer Science and Engineering at North Carolina State University in the United States.

Randy Purse is the Senior Learning Advisor at the Information Technology Security Learning Centre at the Communications Security Establishment in Canada. A former officer in the Canadian Forces, he is an experienced security practitioner and learning specialist. His research interests include the human dimensions of security and collective and transformative learning in the workplace. He has a Master's of Education in Information Technology from Memorial University of Newfoundland in St. John's, Canada, and he is a PhD candidate specializing in Adult and Workplace Learning in the Faculty of Education at the University of Ottawa, Canada.

Acknowledgements

The authors wish to thank Tony Bailetti, George Cybenko, George Dinolt, Risto Rajala, and Mika Westerlund for reviewing and commenting on an earlier draft of this article. We also wish to thank the participants in the multidisciplinary group for their informed engagement.

References

Amoroso, E. 2006. *Cyber Security.* New Jersey: Silicon Press.

Baldwin, D. A. 1997. The Concept of Security. *Review of International Studies,* 23(1): 5-26.

Barabási, A. L., & Albert, R. 1999. Emergence of Scaling in Random Networks. *Science,* 286(5439): 509-512. http://dx.doi.org/10.1126/science.286.5439.509

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

Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. In *Crisis Management: Concepts, Methodologies, Tools and Applications:* 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

Cavelty, M. D. 2008. Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics,* 4(1): 19-36. http://dx.doi.org/10.1300/J516v04n01_03

Cavelty, M. D. 2010. Cyber-Security. In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies:* 154-162. London: Routledge.

Chang, F. R. 2012. Guest Editor's Column. *The Next Wave,* 19(4): 1–2.

CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Cooper, S. 2013. Pragmatic Qualitative Research. In M. Savin-Baden & C. H. Major (Eds.), *Qualitative Research: The Essential Guide to Theory and Practice:* 170-181. London: Routledge.

Deibert, R., & Rohozinski, R. 2010. Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy,* 21(4): 43-57. http://dx.doi.org/10.1353/jod.2010.0010

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014: http://niccs.us-cert.gov/glossary#letter_c

Friedman, A. A., & West, D. M. 2010. Privacy and Security in Cloud Computing. *Issues in Technology Innovation,* 3: 1-13.

Goodall, J. R., Lutters, W. G., & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. *Information Technology & People,* 22(2): 92-108. http://dx.doi.org/10.1108/09593840910962186

ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. 2014. Resource-Based Theory in Marketing. *Journal of Academic Marketing Science,* 42(1): 1-21. http://dx.doi.org/10.1007/s11747-013-0336-7

Kemmerer, R. A. 2003. *Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering:* 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

Lewis, J. A. 2006. *Cybersecurity and Critical Infrastructure Protection.* Washington, DC: Center for Strategic and International Studies. http://csis.org/publication/cybersecurity-and-critical-infrastructure-protection

Defining Cybersecurity

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse

Ostrom, E., & Hess, C. 2007. Private and Common Property Rights. In B. Bouckaert (Ed.), *Encyclopedia of Law & Economics*. Northampton, MA: Edward Elgar.

Oxford University Press. 2014. *Oxford Online Dictionary*. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity

Public Safety Canada. 2010. *Canada's Cyber Security Strategy*. Ottawa: Public Safety Canada, Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Singer, P. W., & Friedman, A. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Public Safety Canada. 2014. *Terminology Bulletin 281: Emergency Management Vocabulary*. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgc-pwgsc.gc.ca/publications/documents/urgence-emergency.pdf

Wallinger, W., Alderson, D., & Doyle, J. 2009. Mathematics and the Internet: A Source of Enormous Confusion and Great Potential. *Notices of the American Mathematical Society,* 56(5): 586-599.

Citation: Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review*, 4(10): 13–21. http://timreview.ca/article/835

Keywords: cybersecurity, definition, interdisciplinary, cyberspace, security