NAAC Accredited
Vidarbha Bahu-uddeshiya Shikshan Sanstha's
TULSIRAMJI GAIKWAD-PATIL
College of Engineering & Technology
DTE CODE 4151
Mohgaon, Wardha Road, Nagpur - 441108 An ISO 9001:2015 Certified Institution
(An Autonomous Institute Affiliated to RTM Nagpur University, Nagpur)

Research on Defining Cybersecurity

Guided By

Prof. Roshan A. Chandekar

Head of Department

M.C.A. Ph.D

Submitted By

Kiran Mahadev Kodape

Prajwal Namdeo Dhawas

Sanket Vikas Pawade

Defining Cybersecurity

Abstract: 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 practitioners, 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.

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; C, 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)

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)

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., 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 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 (venuscyber.com), and graduate students in the Technology Innovation Management program (timprogram.ca) at Carleton University in Ottawa, Canada.

Substantiating 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). 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 cybersecurity 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.

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 BSc and MSc degrees in Mathematics from Carleton University in Ottawa, Canada.

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