Technology Innovation Management Review

November 2014

Image licensed under CC BY-SA Rohit Gowaikar

Cybersecurity

Welcome to the November 2014 issue of the *Technology Innovation Management Review*. This month's editorial theme is Cybersecurity. We welcome your comments on the articles in this issue as well as suggestions for future article topics and issue themes.

Carleton UNIVERSITY

www.timreview.ca

Publisher

The *Technology Innovation Management Review* is a monthly publication of the Talent First Network.

ISSN

1927-0321

Overview

The *Technology Innovation Management Review* (TIM Review) provides insights about the issues and emerging trends relevant to launching and growing technology businesses. The TIM Review focuses on the theories, strategies, and tools that help small and large technology companies succeed.

Our readers are looking for practical ideas they can apply within their own organizations. The TIM Review brings together diverse viewpoints – from academics, entrepreneurs, companies of all sizes, the public sector, the community sector, and others – to bridge the gap between theory and practice. In particular, we focus on the topics of technology and global entrepreneurship in small and large companies.

We welcome input from readers into upcoming themes. Please visit timreview.ca to suggest themes and nominate authors and guest editors.

Contribute

Contribute to the TIM Review in the following ways:

- Read and comment on articles.
- Review the upcoming themes and tell us what topics you would like to see covered.
- Write an article for a future issue; see the author guidelines and editorial process for details.
- Recommend colleagues as authors or guest editors.
- Give feedback on the website or any other aspect of this publication.
- Sponsor or advertise in the TIM Review.
- Tell a friend or colleague about the TIM Review.

Please contact the Editor if you have any questions or comments: timreview.ca/contact

Editorial: Cybersecurity

Chris McPhee, Editor-in-Chief
Tony Bailetti, Guest Editor

From the Editor-in-Chief

Welcome to the November 2014 issue of the *Technology Innovation Management Review*. This is the second of two issues covering the editorial theme of **Cybersecurity**, and I am pleased to welcome back our guest editor, **Tony Bailetti**, Director of Carleton University's Technology Innovation Management program (TIM; timprogram.ca) and Executive Director (Acting) of the VENUS Cybersecurity Corporation (venuscyber.com).

In December, we will be publishing an issue based on our collaboration with the ISPIM Americas conference (americas.ispim.org), which was held in Montreal this past October.

I encourage you to get in touch if you would like to submit an article for a future issue. We hope you enjoy this issue of the TIM Review and will share your comments online. Please contact us (timreview.ca/contact) with article topics and submissions, suggestions for future themes, and any other feedback.

Chris McPhee
Editor-in-Chief

From the Guest Editor

It is my pleasure to be the guest editor for the October and November issues of the TIM Review, in which we explore the theme of Cybersecurity. A total of 20 authors from industry, government, and academia contributed 10 articles, a Q&A, and a summary of a TIM Lecture to these two issues of the TIM Review. These contributions were the outcomes of a capacity-building initiative led by the VENUS Cybersecurity Corporation and Carleton University in Ottawa, Canada. A nationwide effort to make Canada a global leader in cyberspace offers significant benefits to the online users worldwide as well as many opportunities for scholarly inquiry and innovative industrial initiatives.

The November issue of the TIM Review includes six articles. These articles provide a method to assess scientific contributions in cybersecurity; a tool to identify the tasks required to increase the value of a cybersecurity startup through early and rapid globalization; a set of attributes of cyber-attacks; an overview of crimeware marketplaces; a classification that can be used to predict the timing of malware; and an approach to examine the safety domain of the future online world.

Dan Craigen is a Science Advisor at the Communications Security Establishment in Ottawa, Canada. His article first develops an approach to assess scientific contributions and then applies it to assess two contributions to the science of cybersecurity.

Tony Bailetti, a professor from Carleton University, and **Erik Zijdemans**, a master's student at the University of Southern Denmark, provide a tool and illustrate a process to describe, design, challenge, and invent the actions that should be performed to globalize a cybersecurity startup early and rapidly for the purpose of increasing its value.

Mehdi Kadivar, a master's student at Carleton University's Technology Innovation Management program, examines definitions of cyber-attacks published in the literature and information on ten high-profile attacks to identify the attributes of cyber-attacks.

Editorial: Cybersecurity

Chris McPhee and Tony Bailetti

Mahmoud Gad is a PhD candidate in Electrical and Computer Engineering at the University of Ottawa. His article examines the actors, value chains, and modes of operation in underground crimeware marketplaces, and it identifies three facilitating technologies that are likely to significantly expand the reach of cybercriminals.

Brent Maheux, a Senior Software Specialist for the Canadian Government proposes an intention-based classification of malware and merges it with an optimal timing model to help predict the timing of malware based on its classification.

Nadeem Douba is the founding principal at Red Canari Inc., **Björn Rütten** is a Senior Research Associate with The Conference Board of Canada, **David Scheidl** is a recent graduate from Carleton University's Global Politics Program, and **Paul Soble** and **D'Arcy Walsh** are Science Advisors at the Communications Security Establishment. Their article uses a transdisciplinary approach to examine the safety domain of the future online world that can enable humanity to reach profoundly new levels of productivity and creativity.

We hope that you, your colleagues, and your organizations benefit from reading the October and November 2014 issues of the TIM Review.

We thank you for reading the journal and urge you to support initiatives to make the online world safe, productive, and creative for its users.

Tony Bailetti
Guest Editor

About the Editors

Chris McPhee is Editor-in-Chief of the *Technology Innovation Management Review*. Chris holds an MASc degree in Technology Innovation Management from Carleton University in Ottawa and BScH and MSc degrees in Biology from Queen's University in Kingston. He has over 15 years of management, design, and content-development experience in Canada and Scotland, primarily in the science, health, and education sectors. As an advisor and editor, he helps entrepreneurs, executives, and researchers develop and express their ideas.

Tony Bailetti is an Associate Professor in the Sprott School of Business and the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. Professor Bailetti is the Director of Carleton University's Technology Innovation Management (TIM) program. His research, teaching, and community contributions support technology entrepreneurship, regional economic development, and international co-innovation.

Citation: McPhee, C., & Bailetti, T. 2014. Editorial: Cybersecurity. *Technology Innovation Management Review*, 4(11) 3–4. http://timreview.ca/article/843

Keywords: cybersecurity, scientific contributions, science of cybersecurity, startups, globalization, cyber-attacks, crimeware, malware, safety

Assessing Scientific Contributions: A Proposed Framework and Its Application to Cybersecurity

Dan Craigen

> *"The philosophy of science is about as useful to scientists as ornithology is to birds."*
>
> Attributed to Richard P. Feynman (1918–1988)
> Theoretical physicist

Through a synthesis of existing work on evaluating scientific theories and contributions, a framework for assessing scientific contributions is presented. By way of example, the framework is then applied to two contributions to the science of cybersecurity. The science of cybersecurity is slowly emerging. As the science and its theories emerge, it is important to extract the key contributions that characterize actual progress in our understanding of cybersecurity. Researchers and funding agencies will be interested in the assessment framework as a means of assessing scientific contributions to cybersecurity. In a nascent research area such as the science of cybersecurity, this article may contribute to a focused research program to accelerate the growth of the science.

Introduction

Hardly a day goes by without yet another report of significant information security vulnerabilities. Some of the most recent attacks, such as the heartbleed bug (MITRE, 2014a) and the shellshock bug (MITRE, 2014b), have focused on core functionalities. The former vulnerability is in an implementation of an Internet-wide protocol (SSL) and the latter vulnerability is in a widely used UNIX command-line interpreter (bash).

After decades of substantial investment into cybersecurity, it is almost unfathomable that such vulnerabilities continue to expose societies to potentially significant exploitation. In the author's view, the existence of these vulnerabilities reflects the complexity of the cybersecurity space and suggests that the existing paradigms for identifying, responding to, or mitigating vulnerabilities and their potential exploitation are failing. Given the perceived ad hoc nature of cybersecurity, which is usually exemplified by patching systems in response to identified vulnerabilities, there is an emerging belief that the foundations of cybersecurity need to be revisited with a sound theoretical/scientific perspective.

It is through a sound theoretical/scientific perspective that we can evolve cybersecurity from its current (largely) ad hoc nature, to a foundation that is well-principled and informed by scientifically-based tenets (Schneider, 2012). Such a theoretical foundation then informs a rigorous engineering discipline, which, it is hoped, will positively impact cybersecurity postures.

However, a difficulty facing researchers, funding agencies, government, and industry is how to assess putative contributions to such a theory. In this article, we synthesize a framework for assessing scientific contributions to cybersecurity. The framework was motivated by the author's involvement with various initiatives in the science of cybersecurity and the need to ascertain whether contributions were truly progressing and contributing to such a nascent science. Particularly, given that development of such a science will be a multi-decade exercise, being able to measure progress and contributions, at least incrementally, would provide important objective input into both research and funding decisions.

Assessing Scientific Contributions

Dan Craigen

First, we introduce the concept of theory and an approach to building theory. We then review the literature on measuring progress in science and assessing theories. The key concepts arising from the literature are then synthesized into a framework for assessing scientific contributions to cybersecurity. Finally, we demonstrate the use of the framework by applying it to two scientific contributions in cybersecurity.

Building Theories

Theory refers to "a well-confirmed type of explanation of nature, made in a way consistent with the scientific method and fulfilling the criteria required by modern science" (Wikipedia, 2014). Weber (2012) notes that "theories provide a representation of someone's perceptions of how a subset of real-world phenomena should be described" and defines theory as "a particular kind of model that is intended to account for some subset of phenomena in the real world". However, Weber also offered a slightly different definition of theory in an earlier article: "an account that is intended to explain or predict some phenomena that we perceive in the world" (Weber, 2003).

Weber's work builds upon an ontology described by Bunge (1977, 1979), which is used to define theory-related concepts. The key assumptions, as described by Weber (2003), can be summarized as follows:

- The world is perceived as a collection of "things" and "properties of things".
- A state is the values associated with the various properties at a particular time and space.
- Events occur that can result in a change of state.
- Phenomena are defined as states of things or events that occur to things.

Weber (2003) takes the view that "the choice and articulation of the phenomena we are seeking to explain or predict via our theories are the two most-critical tasks we undertake as researchers." A role of a theory is to express "laws" that relate various values of a state. Weber (2003) defines the "account of the phenomena" as "the explanation of the laws that are hypothesized to relate them" and normally uses "constructs," a property of a thing, and association among constructs (a law).

Weber (2012) then introduces the following parts of a theory:

- *Constructs:* represent an attribute (the way we perceive a property)
- *Associations:* for static phenomena, relate construct values; for dynamic phenomena, relate histories of values between constructs
- *States:* identification of state space that is the object of the theory – the range of legal values
- *Events:* identification of the events that are the object of the theory – the range of legal state transitions.

Using these terms, Weber (2012) then discusses how to build a theory:

1. Articulate the constructs of a theory.
2. Articulate the laws of interaction (relationships) among the constructs of a theory.
3. Articulate the lawful state space of a theory.
4. Articulate the lawful event space of a theory.

Although the process is presented linearly, it is important to recognize that theory building is iterative. The process starts with good observations and descriptions, and it improves through inductive/deductive cycles, with anomalies resulting in evolution of the theories. In the early stages of understanding phenomena, it may be necessary to use the theories of other disciplines to first articulate our understandings. As we better comprehend our phenomena, new theories or adapted theories may be developed.

In a similar manner, Sjøberg and colleagues (2008) describe the theory-building enterprise as:

1. Defining the constructs of the theory
2. Defining the propositions of the theory
3. Providing explanations to justify the theory
4. Determining the scope of the theory
5. Testing the theory through empirical research

Assessing Scientific Contributions

Dan Craigen

Measuring Progress in Science

For researchers and funding agencies, it is pertinent to ascertain whether we are making scientific progress: are the scientific contributions meaningful? One key input into such considerations was written by the Committee on Assessing Behavioral and Social Science Research on Aging (Feller & Stern, 2007). Though motivated by research into aging, their characterization of progress transcends the discipline to other scientific endeavours. The committee identified two kinds of progress: i) internally defined (i.e., characterized as intellectual progress and contributions to science), and ii) externally defined (i.e., characterized by contributions to society).

For internally defined progress in science, the committee identified five types of progress:

1. *Discovery:* demonstration of the existence of previously unknown phenomena or relationships among phenomena, or when the discovery that widely shared understandings of phenomena is wrong or incomplete

2. *Analysis:* development of concepts, typologies, frameworks of understanding, methods, techniques, or data that make it possible to uncover phenomena or test explanations of them

3. *Explanation:* discovery of regularities in the ways phenomena change over time or evidence that supports, rules out, or leads to qualifications of possible explanations of these regularities

4. *Integration:* linking theories or explanations across different domains or levels of organization

5. *Development:* stimulation of additional research in a field or discipline, including research critical of past conclusions, and when it stimulates research outside the original field, including interdisciplinary research and research on previously under-researched questions. It also develops when it attracts new people to work on an important research problem.

For externally defined progress in science, the committee identified four types of progress:

1. *Identifying issues:* identifying problems that require societal action or showing that a problem is less serious than previously believed

2. *Finding solutions:* developing ways to address issues or solve problems

3. *Informing choices:* providing accurate and compelling information, thus promoting better informed choices

4. *Educating society:* producing fundamental knowledge and developing frameworks of understanding that are useful for making decisions in the private sector, and participating as citizens in public policy decisions. Science can also contribute by educating the next generation of scientists.

Assessing Theories

Prior to discussing our criteria for assessing contributions to science, we note various criteria that are used to assess theories (Berg, 2009; Cramer, 2013; Sjøberg et al., 2008):

- Testibility; refutability
- Precision
- Empirical validity/support
- Explanatory power; predictability; quantifiable
- Parsimony; consilience; simplicity; self-consistent; rational; inductive
- Generality; comprehensiveness
- Utility; heuristic and applied value
- Repeatability

Weber (2012) uses the ontological structure, briefly discussed above, to evaluate a theory from two perspectives: evaluating the components of a theory and evaluating the whole theory. Weber notes that the components of the theory must be described precisely because they essentially define the domain of the theory. From his perspective, a key advantage of precision is that tests can be better designed.

Weber (2012) evaluates the components of a theory using the following key concepts:

1. *Constructs:* Should be defined precisely; underlying variables clearly identified

Assessing Scientific Contributions

Dan Craigen

2. *Associations:* Described to various levels of precision. With static phenomena, there is a relationship, but no sign; the sign of association between constructs identified; and a functional relationship is described. With dynamic phenomena, there is a relationship, but no sign or direction; the sign of association between constructs identified but not the direction; the direction of association known (implying causality) or time relationship; and a functional relationship identified.

3. *States:* How clear and precise is the description of the state space?

4. *Events:* How clear and precise are the events?

Weber (2012) evaluates a whole theory using the following key concepts:

1. *Importance:* Does the theory address important phenomena from either a practice or research perspective?

2. *Novelty:* Does it resolve anomalies? Does it change research paradigms?

3. *Parsimony:* Is the theory sufficiently simple?

4. *Level:* Is the theory sufficiently abstract? Weber discusses micro-level and macro-level theories, both of which have associated pros and cons.

5. *Falsifiability:* Can the theory be refuted?

Assessing Scientific Contributions

From the above literature review, we synthesize our framework for assessing scientific contributions. There are two aspects to assessing a scientific theory: *Evaluation* and *Contribution*. These two aspects and their components are summarized in Table 1.

Evaluation has two constituents: i) *Well-formedness* and ii) *Testing and Analysis*. Broadly speaking, *Evaluation* refers to expectations of how a theory should be expressed and the means through which the scientific and philosophical communities test and analyze theories for acceptance. In large part, evaluation focuses on technical attributes of the theory.

Contribution has three constituents: i) *Contribution to Science,* ii) *Contribution to Society,* and iii) *Depth of the Contribution*. The first two constituents align directly with the work by the Committee on Assessing Behavioral and Social Science Research on Aging (Feller & Stern, 2007) in that the *Contribution to Science* aligns to a subset of internally defined progress, while *Contribution to Society* aligns to a modified subset of externally defined progress. In large part, contribution focuses on social attributes of the theory – its role within scientific and societal communities.

Evaluation: Well-formedness
In the framework illustrated in Table 1, we identify six attributes to determine if a theory is well-formed:

1. *Components:* Evaluation was discussed by (Weber,

Table 1. Proposed framework for assessing a scientific theory

Evaluation		Contribution		
Well-formedness	**Testing and Analysis**	**Contribution to Science**	**Contribution to Society**	**Depth of the Contribution**
• Components • Precision (Formalism) • Consistency • Completeness • Measurability • Testability	• Falsifiability • Accuracy • Repeatability • Consilience • Parsimony	• Discovery • Analysis • Explanation	• Identifying issues • Finding solutions • Making educated choices	• Generality • Comprehensiveness • Non-obvious results/observations • Novelty

Assessing Scientific Contributions

Dan Craigen

2012), as summarized earlier in this article. We expect each of these components to be present.

2. *Precision (Formalism):* Consistent with Weber, we argue that the components of a theory should be described as precisely as possible. Although natural languages are often used in stylized manners to describe concepts "precisely", the "gold standard" is to describe the components formally using mathematical concepts.

3. *Consistency:* The expression of the theory should be internally consistent; that is, there are no contradictions.

4. *Completeness:* In our context, we view completeness from an "expressively complete" perspective in which the theory can describe all of the properties for which it has been developed.

5. *Measurability:* It should be possible to objectively measure the theory components, particularly the constructs. Key concepts must be quantifiable and the measurements must be objective.

6. *Testability:* The theory components should be amenable to scientific experimentation. This attribute is closely related to both the measurable attribute above and the falsifiable attribute described below.

Evaluation: Testing and Analysis
In Table 1, we identify five attributes for the evaluation of testing and analysis:

1. *Falsifiability:* A key attribute/principle of science – it must be possible to show that the theory is incompatible with possible empirical observations.

2. *Accuracy:* The empirical observations should be in line with the expectations of the theory.

3. Repeatability: The empirical observations should be reproducible.

4. *Consilience:* Evidence from independent, unrelated sources can "converge" to strong conclusions.

5. *Parsimony:* Measures the number of kinds of entities postulated by a theory; theories should be as simple as possible for the phenomena being modelled.

Each of these attributes is testing or analyzing the theory and mostly relate to empirical validation. The first four specifically speak to experiments: Can we fail? Are the experimental results being accurately described or predicted by the theory? Can we repeat the experiment and obtain the same results? Can we obtain the same results by different experimental means? If all of these conditions hold, it then makes sense to ask ourselves whether we have elegance in our theory. Have we truly identified the core relationships and constructs?

Contributions to Science and to Society
The elements *Contribution to Science* and *Contribution to Society* are largely those identified by the Committee on Assessing Behavioral and Social Science Research on Aging (Feller & Stern, 2007). *Contribution to Society* merges their "Informing Choices" and "Education" into *Making Educated Choices* within the proposed framework. Further, for *Contribution to Science,* only the first three attributes are included; development and integration can be viewed as attributes of an *Evaluation of the Contribution.*

As depicted in Table 1, the importance and utility of contributions to science and society are captured in *Evaluation of the Contribution:*

1. *Generality:* Is the scientific contribution of specific or general validity?

2. *Comprehensiveness:* Is the scientific contribution inclusive and of broad scope? Is the scientific contribution inclusive and broadly applicable to societal challenges?

3. *Non-obvious results:* Are there interesting challenges for scientists to explore? Are there unexpected consequences suggested by the theory when contextualized societally?

4. *Novelty:* Does the theory provide new insights otherwise not explored by science? Is it normal science or paradigm changing? Does the theory provide new insights otherwise not explored by society?

Measuring Evaluation

Having defined the various evaluation attributes, we posit some potential values for each of the attributes. For simplicity, we define only three values per attribute:

• Well-formedness

  · Components: all components present; some components present; no components

Assessing Scientific Contributions

Dan Craigen

- · Precision (Formalism): formal/mathematical; semi-formal; informal
- · Consistency: provable consistency; unclear; inconsistent
- · Completeness: provable completeness; unclear; incomplete
- · Measurability: measurable; unclear; not measurable
- · Testability: testable; unclear; not testable

• Testing and analysis

- · Falsifiability: falsifiable; unclear; not-falsifiable
- · Accuracy: accurate; unclear; not-accurate
- · Repeatability: repeatable; unclear; not-repeatable
- · Consilience: consilient; unclear; not-consilient
- · Parsimony: parsimonious; unclear; complex

• Depth of the contributions

- · Generality: general; generalized; specific
- · Comprehensiveness: comprehensive; moderately comprehensive; narrow
- · Non-obvious results/observations: non-obvious; unclear; uninteresting
- · Novelty: paradigm/society shifting; substantive normal progress; not substantive

Applying the Framework

Having defined the framework, we now apply it to two contributions from the science of cybersecurity. These assessments are preliminary, but are intended to illustrate how the framework could be applied.

Phishing in International Waters
At the 2014 Symposium and Bootcamp on the Science of Security (hot-sos.org/2014/), Tembe and colleagues (2014) presented the paper "Phishing in International Waters", in which they reported on a survey of American, Chinese, and Indian Internet users and explored the role of culture in the three nationalities responses to phishing attacks. The authors performed various statistical analyses based on responses to questionnaires and found that there were *cross-national differences in agreement* regarding the characteristics of phishing, the media of phishing, and the consequences of phishing. Conclusions were drawn in part from the individualistic culture represented by Americans and the collectivist cultures represented by China and India.

The statistical analyses included multivariate analysis of covariance and logistic regression analysis. According to the paper, a logistic regression was used to compare nationality with phishing and the characteristics of the risk profile. Further, the authors reported that a multivariate analysis of covariance was used to compare nationality with characteristics of phishing, types of media, and the consequences of phishing. Notably, neither age nor education had any influence on the likelihood of being phished.

Table 2 summarizes our analysis of "Phishing in International Waters" using our framework for assessing scientific contributions.

Selective Interleaving Functions
McLean (2014) presented one of the keynote presentations at the Science of Security conference (HOTSoS, 2014), His presentation, "The Science of Security: Perspectives and Prospects", provided two case studies: one on access control models and the second on information flow models. Here, we assess the scientific contribution of the second case study using our proposed framework. In this second case, McLean examined the evolution of information-flow models and how our understanding in this area has improved over time and has resulted in a compelling framework that could be used to explain information flow models. Table 3 summarizes our analysis of portion of his paper on "Selective Interleaving Functions" and his related earlier paper (McLean, 1994).

Contribution

In this article, we have presented a framework for assessing scientific contributions to cybersecurity and then applied the framework to two contributions to the Science of Cybersecurity. Our assessment framework consists of two parts: Evaluation and Contribution. Through these two parts, we have synthesized and structured a number of approaches cited in the literature for assessing scientific contributions. Prior work, such as that of Weber and the Committee on Assessing Behavioral and Social Science Research on Aging has focused on one part solely (either evaluation or contribu-

Assessing Scientific Contributions

Dan Craigen

Table 2. Assessing the scientific contribution of "Phishing in International Waters" (Tembe et al., 2014) using the proposed framework

Well-formedness		
Components	Some components present	Statistical variables identified
Precision (Formalism)	Semi-formal	Questionnaire used natural language descriptions; statistical analysis is formal
Consistency	Unclear	Further analysis required
Completeness	Incomplete	Probably very difficult to characterize completeness in this case
Measurability	Measurable	The paper identifies measurable criteria through the questionnaire and definition of variables. There are potential biases introduced (as noted by the authors).
Testability	Testable	Variables were identified, a questionnaire defined, responses obtained. In principle, similar surveys could be performed on the same cultures or other cultures (such as European or African cultures – as suggested by the authors).
Testing and Analysis		
Falsifiability	Falsifiable	Hypotheses were not specifically identified, except for the collective/individualistic aspect of the societies.
Accuracy	Unclear	Hypotheses were not specifically identified, except for the collective/individualistic aspect of the societies.
Repeatability	Unclear	While the experiment could be rerun, there has been no demonstration of repeatability.
Consilience	Unclear	No other means of studying the cultural aspects were posited.
Parsimony	Unclear	No comment; insufficient information.
Contributions to Science and Society		
To Science	Explanation	Though an argument could be made that the contribution is analytical, the paper largely explains why Americans, Chinese, and Indians respond differently to phishing attacks.
To Society	Making educated choices	By understanding the cultural nuances of phishing and, as suggested in the paper, by modifying training programs and considering different approaches to security mechanism, the role of culture impacts phishing mitigations.
Depth of the Contributions		
Generality	Specific	The analysis focused on cultural responses to a particular form of attack: phishing.
Comprehensiveness	Narrow	The sample set was small; potential admitted biases from Mechanical Turk
Non-obvious results/observations	Unclear	No relevant comments were provided in the paper
Novelty	Not substantive	While characterized as not substantive, it still demonstrates a multi-disciplinary approach to cybersecurity. It is an early step in understanding cultural attributes of cybersecurity.

Assessing Scientific Contributions

Dan Craigen

Table 3. Assessing the scientific contribution of "Selective Interleaving Functions" (McLean, 2014) using the proposed framework

Well-formedness		
Components	All components present	Not evaluated here
Precision (Formalism)	Formal/mathematical	Not evaluated here
Consistency	Consistent	See McLean (1994) for mathematical presentation
Completeness	Unclear	Not evaluated here
Measurability	Measurable	Systems could be implemented to demonstrate whether, for example, composition claims hold.
Testability	Testable	Systems could be implemented to demonstrate whether, for example, composition claims hold.
Testing and Analysis		
Falsifiability	Falsifiable	Systems could be implemented to demonstrate whether, for example, composition claims hold.
Accuracy	Unclear	Papers cited within are theoretical contributions. While testable and measurable, it is unclear whether any experiments have been performed.
Repeatability	Unclear	Papers cited within are theoretical contributions. While testable and measurable it is unclear whether any experiments have been performed.
Consilience	Unclear	Papers cited within are theoretical contributions. While testable and measurable it is unclear whether any experiments have been performed.
Parsimony	Parsimonious	Selective interleaving functions are effective in unifying information flow models.
Contributions to Science and Society		
To Science	Discovery	McLean argued that selective interleaving functions provided a common framework for an otherwise incomparable collection of information-flow security models. Further benefits arose because they explained why certain types of compositions were harder on security than others.
To Society	Finding solutions	Selective interleaving functions provided an overall characterization of information-flow models and explained difficulties in composability, hence providing information on how systems could be developed with composition in mind.
Evaluation of the Contributions		
Generality	General	Subsumed prior existing work and a miscellaneous collection of information-flow security models. Provided a common framework.
Comprehensiveness	Comprehensive	Within the context of information-flow security models, this approach covers “possibilistic” security properties.
Non-obvious results/observations	Non-obvious	While setting a general framework, it appears this framework also can be used to explore other composition properties.
Novelty	Substantive normal progress	Built upon prior work on understanding safety/liveness, composition theories, etc.

Assessing Scientific Contributions

Dan Craigen

tion). Weber provides a significant assessment of an Information Systems paper that can usefully inform how to proceed with theory evaluations. We expand upon Weber's evaluation by discussing both well-formedness and testing/analyzing criteria a theory more comprehensively.

Particularly, given that development of a Science of Cybersecurity will be a multi-decade exercise, being able to measure progress and contributions, at least incrementally, will provide important objective input into both research and funding decisions and is expected to contribute to a focused research program and accelerate the growth of the science.

Conclusion

The assessment framework presented in this article is preliminary. Specifically, whether the values for each criterion are sensible and whether there should be additional criteria is open for refinement. Weber (2003, 2012) uses an ontological framework to motivate his analysis; future work should build upon these ontological considerations.

Moreover, this type of work can be used to assess "scientific progress". For example, the science of cybersecurity is in its early stages, and it would be beneficial to measure the progress made in the field. Assessing contributions provides potentially rational inputs into the determination of scientific progress and thereby potentially contribute to a focused research program to accelerate the growth of the science.

About the Author

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.

References

Berg, R. 2009. Evaluating Scientific Theories. *Philosophy Now,* 74: 14-17.

Bunge, M. 1977. *Treatise on Basic Philosophy, Volume 3: Ontology I: The Furniture of the World.* Dordrecht, Holland: D. Reidel Publishing Company.

Bunge, M. 1979. *Treatise on Basic Philosophy, Volume 3: Ontology II: A World of Systems.* Dordrecht, Holland: D. Reidel Publishing Company.

Cramer, K. 2013. Six Criteria of a Viable Theory: Putting Reversal Theory to the Test. *Journal of Motivation, Emotion, and Personality,* 1(1): 9-16. http://dx.doi.org/10.12689/jmep.2013.102

Feller, I., & Stern, P. C. (Eds.) 2007. *A Strategy for Assessing Science: Behavioral and Social Research on Aging.* Washington, DC: National Academies Press (US).

McLean, J. 1994. A General Theory of Composition for Trace Sets Closed Under Selective Interleaving Functions. *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy:* 79.

McLean, J. 2014. The Science of Computer Security Perspectives and Prospects. Keynote presentation at the 2014 Symposium and Bootcamp on the Science of Security, April 8-9, Raleigh, NC, United States.

MITRE. 2014a. CVE-2014-0160. *Common Vulnerabilities and Exposures.* November 1, 2014: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

MITRE. 2014b. CVE-2014-7169. *Common Vulnerabilities and Exposures.* November 1, 2014: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169

Sjøberg, D., Dybå, T., Anda, B. C. D., & Hannay, J. E. 2008. *Building Theories in Software Engineering.* In F. Shull, J. Singer, & D. I. K. Sjøberg (Eds.), Guide to Advanced Empirical Software Engineering: 312-336. London: Springer-Verlag. http://dx.doi.org/10.1007/978-1-84800-044-5_12

Tembe, R., Zielinksa, O., Liu, Y., Hong, K. W., Murphy-Hill, E., Mayhorn, C., & Ge, X. 2014. Phishing in International Waters: Exploring Cross-National Differences in Phishing Conceptualizations between Chinese, Indian and American Samples. *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security.* http://dx.doi.org/10.1145/2600176.2600178

Schneider, F. B. 2012. Blueprint for a Science of Cybersecurity. *The Next Wave,* 19(2): 47-57.

Weber, R. 2003. Editor's Comment: Theoretically Speaking. *MIS Quarterly,* 27(3): iii-xii.

Weber, R. 2012. Evaluating and Developing Theories in the Information Systems Discipline. *Journal of the Association for Information Systems,* 13(1): 1-30.

Wikipedia. 2014. Theory. *Wikipedia.* October 1, 2014: http://en.wikipedia.org/wiki/Theory

Citation: Craigen, D. 2014. Assessing Scientific Contributions: A Proposed Framework and Its Application to Cybersecurity. *Technology Innovation Management Review,* 4(11): 5–13. http://timreview.ca/article/844

Keywords: cybersecurity, science of cybersecurity, scientific progress, scientific contributions, societal contributions, assessing science

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

> *"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."*
>
> Newton Lee
> Computer scientist and author

Corporations and government agencies worldwide seek to ensure that their networks are safe from cyber-attacks, and startups are being launched to take advantage of this expanded market for cybersecurity products, services, and solutions. The cybersecurity market is inherently global; therefore, cybersecurity startups must globalize to survive. With this article, we fill a gap in the literature by identifying the factors that make a technology startup valuable to specific stakeholders (e.g., investors, customers, employees) and by providing a tool and illustrating a process to describe, design, challenge, and invent the actions that should be performed to globalize a cybersecurity startup early and rapidly for the purpose of increasing its value. The development of the tool builds on recent advances in the resource-based literature, the review of the literature on born-global firms and business model discovery processes, and the experience gained operating the Lead to Win ecosystem. This article will be of interest to entrepreneurs and their venture teams, investors, business development agencies, advisors, and mentors of cybersecurity startups as well as researchers who develop tools and approaches that are relevant to technology entrepreneurs.

Introduction

Technology startups that globalize early and rapidly are more willing to change and more capable of adapting to uncertain environments (Sapienza et al., 2006), are worth more (Chetty & Campbell-Hunt, 2004), grow revenue and employment faster (Andersson et al., 2004; Gabrielsson & Manek Kirpalani, 2004; Gabrielsson et al., 2004), and bring more cash into a local economy from outside their borders (Poole, 2012). But, how can entrepreneurs discover the actions that should be carried out to make their startups valuable by globalizing early and rapidly? Although the perceived benefits from globalization are known, an approach to systematically describe, design, challenge, and invent the actions that should be performed to make a technology startup valuable by globalizing it early and rapidly is not available.

This article makes two contributions. First, it combines the ex-ante value of a resource and born-global literature streams in the development of a tool that can help technology startups increase their value. Second, the article provides entrepreneurs with a means to identify the specific and concrete actions that should be performed to globalize their startups early and rapidly.

In the remainder of this article, we first identify what makes a technology startup valuable and what enables a technology startup to globalize early and rapidly. Then, we develop a tool, the Global Value Generator, we illustrate the process to generate the actions that can help globalize a technology startup, and we identify generic examples of the actions that 12 existing cybersecurity startups have carried out to globalize. The last section provides the conclusions.

To Make a Technology Startup Valuable

We identify the conditions that make a technology startup valuable to a stakeholder ex-ante (i.e., value of the startup is based on forecasts and not the results of the startup's performance). Traditionally, the resource-

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

based literature posits that superior performance over other firms is a direct result of the access to and use of superior resources (Barney, 1991; Peteraf, 1993; Simon et al., 2007).

Schmidt and Keil (2012) develop a theory that identifies the ex-ante conditions under which firms attribute value to a resource. They highlight the crucial difference between the ex-ante value of a resource (i.e., value before a decision to acquire or build the resource is made) and the ex-post value of a resource (i.e., value after the performance of the resource is known). Schmidt and Keil also identify four conditions that make a resource valuable to a firm ex-ante: i) the firm's ex-ante market position; ii) its ex-ante resource base, which allows for complementarities; iii) its position in inter-organizational networks; and iv) the prior knowledge and experience of its managers.

We apply the logic that Schmidt and Keil (2012) used to examine the ex-ante value a firm allocates to a resource for the purpose of examining the ex-ante value a stakeholder allocates to a technology startup. A stakeholder is an individual or organization that can potentially make cash or in-kind contributions to the startup. In-kind contributions can include access to resources and people.

We postulate that, to increase its ex-ante value to a stakeholder, a technology startup must act to:

1. *Increase spread:* Increase the spread between customers' willingness to pay for its product and the cost of the product

2. *Increase demand:* Increase the demand for its product

3. *Increase complementarity:* Increase the demand for the stakeholder's products complemented by the startup's product

4. *Increase privileged information:* Establish a position in inter-organizational networks that improves the volume, variety, velocity, and veracity of privileged information that is accessible

5. *Increase judgment:* Attract individuals who have the requisite experience and knowledge to create value for the startup

A stakeholder, while making decisions about the value of a startup, will develop forecasts for the results from the five actions identified above. The results of carrying out these five actions will determine how much value a stakeholder attributes to a technology startup. The value of a startup is idiosyncratic to the stakeholder; even when all stakeholders have the same information they will attribute different values to the startup.

A key result of applying Schmidt and Kiel (2012) is that the ex-ante value of a technology startup is driven by forecasts of product market value creation that is made possible by the startup's existence, not just the startup's ability to generate profitable revenue. Forecasts of "increased spread" and "increased demand" express the startup's ability to increase its revenue. Forecasts of "increased complementarity", "increased privileged information", and "increased judgment" express other components of product market creation that the startup is expected to enable.

To Enable Early and Rapid Globalization in a Technology Startup

We reviewed the born-global literature to identify the factors that enable a technology startup to globalize early and rapidly. We found that startups that globalize early and rapidly tend to take the following actions:

- Use the Internet intensively (Jaw & Chen, 2006; Maltby, 2012, Tanev, 2012; Yoos, 2013)

- Partner with companies with a global footprint (Lemminger et al., 2014; Nummela et al., 2014)

- Have top managers with international experience (Hutchinson et al., 2007; Kudina et al., 2008; Poole, 2012; Sapienza et al., 2006; Spence & Crick, 2009)

- Trade control for growth (Spence & Crick, 2009)

- Develop niche products with global appeal (Spence & Crick, 2009; Chetty & Campbell-Hunt, 2004; Hutchinson et al., 2007; Kudina et al., 2008)

- Initially focus on selling in the lead market for their technology regardless of geographic location (Knight et al., 2004; Spence & Crick, 2009)

- Develop a strong brand identity (Hutchinson et al., 2007)

- Identify international opportunities (Karra et al., 2008)

- Focus on customers with overseas operations (Kudina et al., 2008)

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

We reduce this born-global literature into its individual constituents and postulate that the factors that enable a technology startup to globalize early and rapidly are:

1. *Niche market on 2+ continents:* address the needs of one niche market with technology development, sales channels, and online business processes on at least two continents

2. *2+ Global customers:* sell to at least two customers that have global footprints

3. *1+ global partner:* partner with at least one organization that has a global footprint

4. *Top manager experience on 2+ continents:* ensure that the top management team has work experience and networks on at least two continents

5. *Stakeholders on 2+ continents:* attract customers, partners, investors, and board of directors members who are based on at least two continents

6. *Memberships in commerce organizations on 2+ continents:* maintain active memberships in commerce organizations (e.g., chambers of commerce) on at least two continents, and publish press releases that originate from those continents

Global Value Generator and Search Process

Table 1 provides a tool in the form of a matrix that combines the five factors that enable a technology startup to be valuable and the six factors that enable a technology startup to globalize early and rapidly.

We believe that the Global Value Generator shown as Table 1 can be used by entrepreneurs to anchor the search for actions illustrated in Figure 1. The purpose of the search is to identify and test the specific and concrete actions that a technology startup should carry out to make it valuable by globalizing early and rapidly.

The discovery of the actions to increase the value of a technology startup by globalizing early and rapidly

Table 1. Global Value Generator

To Globalize Early and Rapidly	**To Make a Technology Startup Valuable**				
	Increase spread	Increase demand	Increase complementarity	Increase privileged information	Increase judgment
Niche market on 2+ continents					
2+ Global customers					
1+ global partner					
Top manager experience on 2+ continents					
Stakeholders on 2+ continents					
Memberships in commerce organizations on 2+ continents					

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

should be a disciplined process that is carried out during the early stage of a startup's lifecycle. Muegge (2012) argues that a disciplined discovery process is one that is designed to enable opportunities for learning to arise and has a work plan that results in specific deliverables.

Each cell in Table 1 identifies assertions about the actions that should be carried out. Each assertion included in one of the cells in Table 1 is a cause-effect statement about what a technology startup will do to globalize early and rapidly and what will happen to the factors that drive value as a result. The structure of the statement is as follows: If a startup does "X" to globalize early and rapidly, then "Y" will be the value result). Each statement must be clear, short, simple, and concise. The assertions build on prior knowledge, logical inference, and informed, creative imagination.

Figure 1 illustrates the search process anchored around the use of the Global Value Generator. The first step is to populate the cells in Table 1 with initial assertions. Then, in the second step, new assertions are added and existing assertions are modified, detailed, or eliminated. In the third step, a lean process is used to test the assertions. This process should be a quickly iterating cycle that continuously states and validates assertions with stakeholders and learns from the past. Assertions that stakeholders validate can be refined. Assertions that stakeholders do not validate are modified or eliminated. The fourth step is to identify a set of actions that, as a whole, will produce requisite results at an acceptable level of confidence.

The process illustrated in Figure 1 allows a technology startup to describe the actions they take in their globalization process, as well as design, challenge, and invent specific and concrete actions. Muegge (2012) provides the rationale for using a disciplined model discovery process such as the one illustrated in Figure 1. He emphasizes that discipline has two components: intent and structure. Technology entrepreneurs should deliberately identify and undertake activities to acquire new information, test assumptions, and uncover new options and organize discovery-driven activities as a project, with beginning and end points in time, specific deliverables, and a work plan to produce those deliverables.

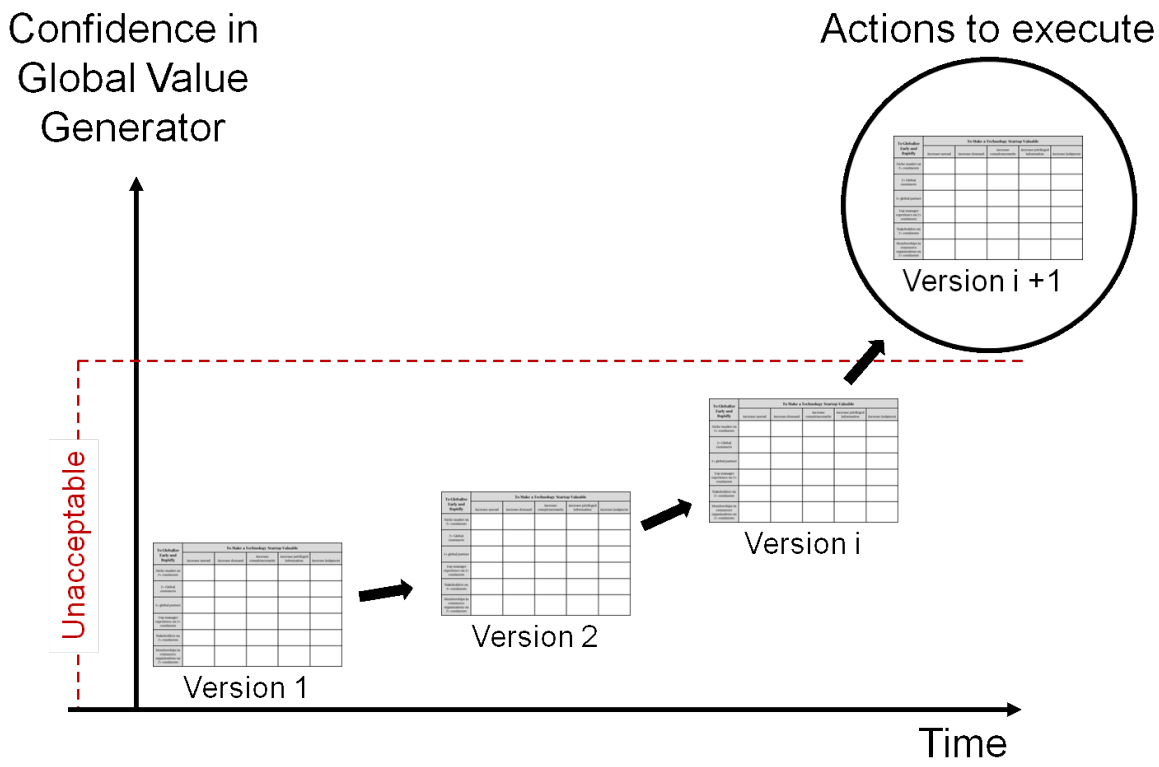

Figure 1. Illustration of the disciplined discovery process that leads to the identification of actions to globalize early and rapidly

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

Examples of Actions Cybersecurity Startups Carry Out to Globalize

The websites of 12 cybersecurity startups that are based in North America and have been operating for five years or less were examined for the purpose of providing generic examples of the actions that firms that operate in the cybersecurity market carry out to globalize early and rapidly. The startups were identified by two experts who work to secure the networks of the federal government of Canada and have experience with suppliers of cybersecurity products and services. We made no attempt to select startups judged to be successful because of these actions.

For each startup, we first used the information provided on its website to infer the actions undertaken to globalize and then these actions were organized into the cells included in the Global Value Generator (Table 1). This activity resulted in 12 matrices: one for each startup. Finally, we collapsed the information in the cells of the 12 matrices into the cells of one matrix.

The 12 startups examined currently operate in the following eight cybersecurity product markets:

1. Total cybersecurity solutions for specific global industries such as aerospace and defense

2. Digital identity and information security and assurance

3. Automated threat forensics and dynamic malware protection

4. Secured distribution

5. Integrated products and services

6. Password-protected login security

7. Simulation software and associated design, testing, and certification services

8. Training, consultancy, and project management

Table 2 provides the information that was collapsed from the 12 matrices (i.e., the actions we inferred that the startups carried out to globalize). The sole purpose of producing Table 2 was to provide generic examples of actions undertaken by cybersecurity startups to globalize. The decisions as to the cells where these examples are shown in Table 2 were made by the authors solely for the purpose to illustrate what the high level results of a discovery process may look like.

The objective of an entrepreneur using the tool introduced in Table 1 as part of a disciplined discovery process is to identify a set of actions that are specific and concrete. By specific actions, we mean those that apply to a particular cybersecurity startup and are not generic like those provided as examples in Table 2. By concrete actions we mean those that are results oriented, not abstract.

Conclusion

The main motivation for writing this article was to provide a tool that can help entrepreneurs discover the actions that they should carry out to increase the exante value of their cybersecurity startups through early and rapid globalization. The tool was developed by leveraging a recent theoretical advance in resource-based theory (Schmidt & Keil, 2012), a review of the born-global literature, research on business model discovery (Muegge, 2012), and the experience gained operating the Lead to Win ecosystem (leadtowin.ca) (Bailetti & Bot, 2013).

In this article, five factors that make a technology startup valuable were identified by applying the logic that Schmidt and Kiel (2012) used to advance the resource-based theory. Moreover, six factors that enable a technology startup to globalize early and rapidly were identified from a literature review. These factors were combined into the Global Value Generator, a tool structured as a matrix that can be used to describe, design, challenge, and invent the specific and concrete actions that a cybersecurity startup should perform for the purpose of increasing its value by globalizing early and rapidly. The Global Value Generator needs to be used as part of disciplined discovery processes such as the one described by Muegge (2012). The tool can be used to complement the various business model frameworks proposed in both the management literature and consulting organizations.

We offer three questions to anchor future research efforts. The first research question is: What are the specific actions to globalize early and rapidly that have the greatest effect on the value of the cybersecurity startups? The relationship between the specific actions to globalize and the value of the startup needs to be examined empirically. This effort requires that a myriad of definitional issues be resolved and will take years to complete.

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

Table 2. Examples of actions a cybersecurity startup may carry out to increase its value by globalizing early and rapidly

To Globalize Early and Rapidly	To Make a Technology Startup Valuable				
	Increase spread	Increase demand	Increase complementarity	Increase privileged information	Increase judgment
Niche market on 2+ continents	Target a niche market where customers have a distinct set of cybersecurity needs and are willing to pay a premium price	Use the Internet as a global sales channel to double product demand	Develop a product that complements products offered by incumbents	Engage with members of virtual communities that attract customers and competitors	
2+ Global customers	Target customers with a global footprint that are willing to pay a premium to solve their cybersecurity problems	Target customers that are members of global supply chains and use their networks to identify the need for security solutions of their partners	Develop security solutions that add value to a customer's products or services that are sold worldwide	Establish relationships with organizations that provide information to customers	Create a network of evangelists among global customers
1+ global partner	Actively participate in the development of global standards on security requirements with global partners	Target partners with a global footprint to increase global demand for startup's product	Target partners who would benefit from the complementarity of the startup's product or service	Use connections to partners to increase access to privileged information	Seek partners with global reach
Top manager experience on 2+ continents	Use top management's intercontinental experience and networks to decrease the cost of rapid globalization	Use top management's intercontinental experience and networks to increase demand	Use top managers with experience in the market whose products/services the startup complements	Use top management's intercontinental networks to increase the access to privileged information	Attract top managers with intercontinental work experience in cybersecurity-related fields
Stakeholders on 2+ continents	Use stakeholders' intercontinental experience and networks to decrease the cost of rapid globalization	Use stakeholders' intercontinental experience and networks to increase demand	Use stakeholders on different continents to identify the geo-political differences that could shape the development of complementary products and services	Use stakeholders' intercontinental networks to increase the access to privileged information	Attract Board of Directors members with knowledge and expertise in cybersecurity-related fields on different continents
Memberships in commerce organizations on 2+ continents	Create exposure in worldwide media renowned for cybersecurity coverage to increase customers' willingness to pay	Create exposure in worldwide media renowned for cybersecurity coverage to increase global demand	Use memberships to identify partners and complementary products and services	Use memberships in commercial associations to increase access to privileged information	Attract Board of Directors members who are also active in commerce organizations

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

The second question is: What actions to globalize early and rapidly are unique to cybersecurity startups? The objective of this research would be to identify the specific actions that startups that depend on the existence of a global resource such as cyberspace need to do that other born-global firms do not. For example, cybersecurity startups can and perhaps should issue specific "threat-scapes" for the global markets they target. This action would be unique to cybersecurity firms. Managerial judgment and imagination about how a cybersecurity startup can help create value for customers worldwide may be key factors that drive its value.

The third research question is: How can business development agencies improve the support they provide to cybersecurity ventures? Hundreds of incubators and accelerators for startups operate worldwide. They address the needs of startups that operate in many different product markets. The objective of this research would be to identify the tools, processes, simulations, and so on required to better support the startups that operate in the cybersecurity domain. For example, what can business development agencies do to support startups that wish to issue threat-scapes for global markets, improve their managerial judgment, and imagine solutions to specific cybersecurity problems of customers worldwide?

About the Authors

Tony Bailetti is the Director of Carleton University's Technology Innovation Management (TIM) program in Ottawa, Canada. His research, teaching, and community contributions support technology entrepreneurship, regional economic development, and the early and rapid globalization of technology ventures.

Erik Alexander Zijdemans is a Master's degree candidate in Product Development and Innovation with a focus on Global Supply Chain Development at the University of Southern Denmark in Odense. He holds a BEng in Business Engineering from Hogeschool Utrecht, The Netherlands. Currently, he is conducting his research on the role of business development agencies in the support of early globalization in technology startups at Carleton University in Ottawa, Canada.

References

Andersson, S., Gabrielsson, J., & Wictor, I. 2004. International Activities in Small Firms: Examining Factors Influencing the Internationalization and Export Growth of Small Firms. *Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration*, 21(1): 22-34. http://dx.doi.org/10.1111/j.1936-4490.2004.tb00320.x

Bailetti, T., & Bot, S. D. 2013. An Ecosystem-Based Job-Creation Engine Fuelled by Technology Entrepreneurs. *Technology Innovation Management Review*, 3(2): 31-40. http://timreview.ca/article/658

Barney, J. B. 1991. Firm Resources and Sustained Competitive Advantage. *Journal of Management,* 17(1): 99-120. http://dx.doi.org/10.1177/014920639101700108

Chetty, S., & Campbell-Hunt, C. 2004. A Strategic Approach to Internationalization: A Traditional versus a "Born-Global" Approach. *Journal of International Marketing*, 12(1): 57-81. http://dx.doi.org/10.1509/jimk.12.1.57.25651

Gabrielsson, M., & Manek Kirpalani, V. H. 2004. Born Globals: How to Reach New Business Space Rapidly. *International Business Review,* 13(5): 555-571. http://dx.doi.org/10.1016/j.ibusrev.2004.03.005

Gabrielsson, M., Sasi, V., & Darling, J. 2004. Finance Strategies of Rapidly-growing Finnish SMEs: Born Internationals and Born Globals. *European Business Review,* 16(6): 590-604. http://dx.doi.org/10.1108/09555340410565413

Hutchinson, K., Alexander, N., Quinn, B., & Doherty, A. M. 2007. Internationalization Motives and Facilitating Factors: Qualitative Evidence from Smaller Specialist Retailers. *Journal of International Marketing,* 15(3): 96-122. http://dx.doi.org/10.1509/jimk.15.3.96

Jaw, Y.-L., & Chen, C.-L. 2006. The Influence of the Internet in the Internationalization of SMEs in Taiwan. *Human Systems Management,* 25(3): 167-183. http://iospress.metapress.com/content/18x6y4kt4e414m20/

Karra, N., Phillips, N., & Tracey, P. 2008. Building the Born Global Firm: Developing Entrepreneurial Capabilities for International New Venture Success. *Long Range Planning*, 41(4): 440-458. http://dx.doi.org/10.1016/j.lrp.2008.05.002

Knight, G., Madsen, T. K., & Servais, P. 2004. An Inquiry into Born-Global Firms in Europe and the USA. *International Marketing Review,* 21(6): 645-665. http://dx.doi.org/10.1108/02651330410568060

Kudina, A., Yip, G. S., & Barkema, H. G. 2008. Born Global. *Business Strategy Review*, 19(4): 38-44. http://dx.doi.org/10.1111/j.1467-8616.2008.00562.x

Lemminger, R., Svendsen, L., Zijdemans, E., Rasmussen, E., & Tanev, S. 2014. Lean and Global Technology Start-ups: Linking the Two Research Streams. The ISPIM Americas Innovation Forum 2014. Montreal, Canada.

Maltby, T. 2012. Using Social Media to Accelerate the Internationalization of Startups from Inception. *Technology Innovation Management Review*, 2(10): 22-26. http://timreview.ca/article/616

Cybersecurity Startups: The Importance of Early and Rapid Globalization

Tony Bailetti and Erik Zijdemans

Muegge, S. 2012. Business Model Discovery by Technology Entrepreneurs. *Technology Innovation Management Review,* 2(4): 5-16.
http://timreview.ca/article/545

Nummela, N., Saarenketo, S., Jokela, P., & Loane, S. 2014. Strategic Decision-Making of a Born Global: A Comparative Study From Three Small Open Economies. *Management International Review,* 54(4): 527-550.
http://dx.doi.org/10.1007/s11575-014-0211-x

Peteraf, M. A. 1993. The Cornerstone of Competitive Advantage: A Resource-Based View. *Strategic Management Journal,* 14(3): 179-191.
http://dx.doi.org/10.1002/smj.4250140303

Poole, R. 2012. Global Mindset: An Entrepreneur's Perspective on the Born-Global Approach. *Technology Innovation Management Review,* 2(10): 27-31.
http://timreview.ca/article/617

Sapienza, H. J., Autio, E., George, G., & Zahra, S. A. 2006. A Capabilities Perspective on the Effects of Early Internationalization on Firm Survival and Growth. *Academy of Management Review,* 31(4): 914-933.
http://dx.doi.org/10.5465/AMR.2006.22527465

Schmidt, J., & Keil, T. 2012. What Makes a Resource Valuable? Identifying the Drivers of Firm-idiosyncratic Resource Value. *Academy of Management Review,* 38(2): 206-228.
http://dx.doi.org/10.5465/amr.10.0404

Sirmon, D. G., Hitt, M. A., & Ireland, R. D. 2007. Managing Firm Resources in Dynamic Environments to Create Value: Looking Inside the Black Box. *Academy of Management Review,* 32(1): 273-292.
http://dx.doi.org/10.5465/AMR.2007.23466005

Spence, M., & Crick, D. 2009. An Exploratory Study of Canadian International New Venture Firms' Development in Overseas Markets. *Qualitative Market Research: An International Journal,* 12(2): 208-233.
http://dx.doi.org/10.1108/13522750910948798

Tanev, S. 2012. Global from the Start: The Characteristics of Born-Global Firms in the Technology Sector. *Technology Innovation Management Review,* 2(3): 5-8.
http://timreview.ca/article/532

Yoos, S. 2013. Market Channels of Technology Startups that Internationalize Rapidly from Inception. *Technology Innovation Management Review,* 3(10): 32-37.
http://timreview.ca/article/618

Citation: Bailetti, T., & Zijdemans, E. 2014. Cybersecurity Startups: The Importance of Early and Rapid Globalization. *Technology Innovation Management Review,* 4(11): 14–21. http://timreview.ca/article/845

Keywords: cybersecurity, born global, startups, globalization

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

Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

> *"The cause is hidden. The effect is visible to all."*
>
> Publius Ovidius Naso (43 BC – AD 17/18)
> Poet

The cybercrime community has evolved from one in which criminals develop their own tools into one in which crimeware – tools and services to carry out or facilitate illegal online activity – can be readily bought, sold, traded, hired, or licensed in online marketplaces. Crimeware marketplaces are expected to grow significantly in the near term, and they will offer an increasing number of services and tools that target mobile computing devices. This article examines the actors, value chains, and modes of operation in underground crimeware marketplaces, and it identifies three facilitating technologies that are likely to significantly expand the reach of cybercriminals. Anonymous e-currency (e.g., Bitcoin) enables anonymous financial transactions; anonymity networks (e.g., Tor) enable anonymous Internet access; and mobile computing provides access to a very large number of potential target devices.

Introduction

Over the past 20 years, the degree of sophistication of cybercrimes has increased while the knowledge of the typical intruder has decreased (Ablon et al., 2014). How is it that more sophisticated crimes are being committed by less sophisticated criminals? These seemingly paradoxical trends may be a direct result of value chains anchored on crimeware marketplaces.

Today, online marketplaces exist where participants use web-based platforms to meet, discuss, exchange, and buy and sell goods and services to enable cybercrime activities (Goncharov, 2012, 2014; Holt, 2013; Kraemer-Mbulaa et al., 2013; Lusthaus, 2013). These crimeware marketplaces provide an easy way to find co-offenders, keep up to date on current cybercrime practices, and coordinate actions to gain competitive advantages in specific market niches (Lusthaus, 2013).

Cybercrime refers to a criminal offence involving a computer as the object of the crime (e.g., computer hacking and unauthorized use of computer systems) or as the tool used to commit a material component of the offence (e.g., credit card fraud and identity theft perpetrated over the Internet) (Kowalski, 2002). The global annual cost of cybercrime is estimated to be between $0.3 and $1 trillion USD, which represents 0.4% to 1.4% of the global gross domestic product (McAfee, 2013, 2014).

Cybercrime supports underground economies in both developed and developing countries worldwide. The United States is considered the major generator of malware and the source of most cybercriminal attacks (Kraemer-Mbulaa et al., 2013), and several studies have examined crimeware marketplaces in the United States. For example, Thomas and Martin (2006) studied a marketplace specialized in financial fraud that leveraged the Internet Relay Chat (IRC) protocol. Franklin, Paxson, Perrig, and Savage (2007) were the first to empirically monitor and analyze the underground economy. China is also considered a major cybercrime hub, while Russia is considered to be the birthplace of cybercrime (Symantec, 2008; Goncharov, 2012). Recently, Brazil has emerged as a new player on the global cybercrime stage and its hackers have become known for financial frauds (Kshetri, 2010).

In this article, the actors, value chains, modes of operation, and mediums of exchange related to crimeware marketplaces are discussed. Then, three facilitating

Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

technologies that enable the growth of cybercrime marketplaces in the near future are identified. Finally, the last section provides the conclusions.

Crimeware Marketplaces

Cybercriminals rely on marketplaces much in the same way as legitimate businesses (Kraemer-Mbulaa et al., 2013). Cybercriminals have different computer skills as well as different motivations. Crimeware marketplaces enable specialization: a computer programmer can code a malware and sell it without becoming involved in the cybercrime operations and details. Crimeware marketplaces also lower the amount of technical skills required to enter the cybercrime world by providing low-skilled cybercriminals with all the necessary tools and support to commit their crimes. These marketplaces enable criminals to develop new hacking tools, recruit and retain talented individuals, develop required skills, and distribute the proceeds of crime among organizations (McAfee, 2013; Sood & Enbody, 2013). Examples of crimeware marketplaces places are listed below; further example can be found at DeepDot Web (tinyurl.com/lnlyzam):

1. *Evolution:* a marketplace for malware, credit card data, distributed denial-of-service (DDoS) attacks, and hacked accounts with a full-functioning automatic escrow system

2. *HPC:* a forum for Russian-speaking hackers with a marketplace section for buying and selling hacking tools and services

3. *Rescator:* an online market for buying and selling stolen credit cards

A number of high profile underground marketplaces were targeted by law enforcement agencies in United States and Europe in the past two years. The Silk Road marketplace, an underground marketplace for drugs, stolen credit cards, and other crimeware, was shut down by the Federal Bureau of Investigation in the United States in late 2013 (Zetter, 2013). Silk Road 2.0, along with 413 other underground marketplaces, were shut down in a joint operation between law enforcement agencies from 17 countries in late 2014 (Fox-Brewster, 2014). It is expected that the future of these markets is not centralized sites like Silk Road, but sites where listings, messaging, payment and feedback are all separated, controlled by no central party and thus very hard for law enforcement agencies to shut down (The Economist, 2014).

Key Elements

In this section, three key elements of underground marketplaces are discussed: i) actors, ii) value chains, and iii) modes of operation.

Actors

Ablon, Libicki and Golay (2014) studied different crimeware marketplaces and they identified three main actors that operate in typical crimeware marketplaces:

1. *Subject-matter experts and administrators:* elite security researchers, exploit developers, malware coders, identity collectors, programmers, and technology experts who research, develop, and support innovative ideas and products in cybercrime marketplaces. They possess sophisticated technical skills and they operate as wholesale sellers to other vendors.

2. *Vendors:* crimeware operators such as crime-as-a-service providers, spammers, botnet owners, drop-service providers, distributors, and ID/financial data providers. They can be technically sophisticated or not, depending on the type of the product or the service they are selling.

3. *General members:* generally buyers and sometimes observers who visit those marketplaces for research, learning, or out of curiosity. They are typically the least technically skilled of the three actors.

Value chains

A value chain refers to the activities carried out to deliver a valuable product or service for a market (Porter, 1985). The value chain is a key concept in legitimate businesses as well as criminal communities.

Kramer-Mbulaa, Tangb, and Rusha (2013) identified three core activities in the value chains designed to carry out credit card fraud: i) the detection of vulnerabilities in a digital system, ii) the distribution of malware, and iii) the exploitation of network vulnerabilities. Each of these activities is typically carried out by a specialized group. The first activity is carried out by professional hackers and it is considered as the most technically complex. The second activity is carried out by sellers of malicious software in online marketplaces. The third activity is carried out by criminal gangs, and it is considered to be the least complex.

Modes of operation

This section reviews five cybercrime modes of operation facilitated by crimeware marketplaces.

Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

1. *Crimeware-as-a-Service (CaaS):* the rental of malware, computing resources, and hosting services to commit cybercrimes (Sood & Enbody, 2013). CaaS customers do not require technical knowledge to launch an attack. Instead, a CaaS provider will attack a website on behalf of the customer, who need only identify a target, specify the type of service, and provide payment. The wide range of available services includes highly specialized password cracking, distributed denial-of-service (DDoS) attacks, and email spam.

2. *Pay-per-install:* cybercriminals may choose to outsource the distribution process of their malware applications to a third party. They provide this third party with the malware and how many targets they need to infect and pay them based on the final number of infected targets (Caballero et al., 2011).

3. *Crimeware toolkits:* "how-to" software packages that instruct users on how to infect a system and then retrieve data, such as corporate documents, personal photos, or credit card information, for financial gain. These off-the-shelf tools minimize the user's need for programming skills (Ben-Itzhak, 2009).

4. *Brokerage:* brokers act as a trusted intermediary between a seller and buyer of malware, stolen credit cards, or other illegal services (Holt, 2013). Trust between buyers and sellers is an issue in crimeware marketplaces, where there is no easy way to check the quality of the "product" or the "service" before completing the transaction. The brokerage operation mode emerged to partially fill this gap. As an example, in marketplaces for stolen credit cards, the broker will be one of the marketplace founders or operators who will hold the money from the buyer in a trust until the stolen credit card information, such as the card number, name on the card, etc., are verified by the broker and delivered to the buyer. The broker will then release the money to the seller in exchange for a brokerage fee.

5. *Data supplier:* data types include password lists, large spam email databases, medical records, driving license numbers, and corporate information are typical data that can be found in underground markets. Cybercriminals operate servers that are used as "drop sites" for private information harvested using malware.

Facilitating Technologies in Crimeware Marketplaces

In this section, we identify three facilitating technologies in crimeware marketplaces: anonymous e-currency (e.g., Bitcoin), anonymity networks (e.g., Tor), and mobile computing technology. The first two technologies enable anonymous financial transactions and anonymous Internet access, which are highly valued features for cybercriminals. The more these technologies become adopted in crimeware marketplaces, the harder it will be for law enforcement agencies to fight back against cybercrime. The third technology opened a large pool of cybercrime targets compared to the classical personal computing platforms.

Anonymous e-currency

Underground businesses typically use e-currency as a medium to instantaneously exchange money and avoid being tracked by law enforcement agencies. There are many e-currencies available in the market, such as Liberty Reserve, e-gold, WM Transfer, virtual gift cards, and prepaid phone cards. For an e-currency to be a successful option in underground marketplaces, its transactions should be internationally accepted, anonymous, irreversible, and unregulated (Lovet, 2006). However, at some point, cybercriminals must convert their profits into real currency, and there are service providers available to solve this problem. E-currency exchange providers charge fees to cash-out e-currencies based on the amount of a transaction and whether or not it involves the purchase of goods (Ablon et al., 2014).

Anonymous e-currency is a class of e-currency that provides anonymity to both buyers and sellers. Currently, the anonymous currencies market is dominated by Bitcoin, a software-based payment system introduced first as a concept in 2008 (Nakamoto, 2008) and then as open source software in 2009. Since then, the use of Bitcoin in online crimeware marketplaces has grown rapidly to the point that it now dominates all other payment methods in terms of adoption and volumes of transactions in most crimeware marketplaces (Ablon et al., 2014). Payments are processed and recorded on peer-to-peer basis without the need for a central repository or a single administrator. Although its status as a currency is disputed – the Internal Revenue Service in the United States considers it a commodity rather than a currency (Internal Revenue Service, 2014) – media reports often refer to Bitcoin as digital currency (Van Name, 2014).

Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

Bitcoin offers all the four properties of an e-currency (internationally accepted, anonymous, irreversible, and unregulated) in addition to being independent from an issuing entity. Bitcoin is not issued by a central bank and it is not being operated by a company. With these unique properties, Bitcoin is the only anonymous and widely accepted e-currency in crimeware marketplaces. Currently, a growing number of legitimate businesses have started to accept Bitcoin as a method of payment. Bitcoin is also used in different illegal online marketplaces outside of cybercriminal marketplaces. For example, Bitcoin was the preferred method of payment for the original Silk Road marketplace and Silk Road 2.0.

The anonymity and the growing adoption of Bitcoin make it very challenging for law enforcement agencies to track (Ablon et al., 2014). A request for vendors to conduct research on how BitCoin can pose threats to national security has recently been issued by the United States (United States, Department of the Navy, 2014).

Due to the anonymity feature of Bitcoin, it is technically very hard for law-enforcement agencies to prevent their misuse. However, at some point, a Bitcoin holder will need to cash their Bitcoins into real money or services. New regulations can be implemented at these "exit points". It may be possible to impose the same federal electronic-fund reporting limits imposed on cash and bank transfers, on e-currencies exchanges especially at the cash out point, such as Bitcoin to cash ATMs.

Anonymity networks

Anonymity networks enable anonymous and untraceable access to the Internet. Tor, which stands for "The Onion Router", is the most widely adopted such technology. Tor is an open source project to enable online anonymity and resist censorship. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays for the purpose of concealing a user's location or usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user, including visits to websites, online posts, instant messages, and other communication forms.

Tor networks enable the operation of anonymous website hosting and file sharing, and when combined with Bitcoin, they enable anonymous marketplaces for different criminal activities, including crimeware marketplaces. These un-indexed webpages exist in the Deep Web and operate as the previously discussed crimeware marketplaces but with an added layer of anonymity protection.

Mobile computing devices

The sales of personal computers have declined while the sales of mobile devices for both work and personal use have increased (Sher & Ovide, 2013; Gartner, 2013). This change in consumer preferences is reflected in the cybercriminal underground economy. This sharp increase in mobile devices sales increases the number of targets available to cybercriminals. According to a Gartner's report on the mobile phone market (Atwal et al., 2013), the Android operating system was installed on 78.4% of the one billion mobile phones sold worldwide in 2013. Because of Android's quick and wide-scale adoption, it has become the target of malicious applications, which continue to increase in number (Jianwei et al., 2012). This shift towards mobile computing devices is alarming to the cybersecurity community. Yu (2013) expects an increase in the number of available malware applications in online underground marketplaces that are specifically designed for mobile devices.

Prevalence of facilitating technologies

The SERT Quarterly Threat Intelligence Report (2013) shows an increase of 350% in Tor traffic in the third quarter of 2013. This increase is believed to be in part due to privacy concerns after Edward Snowden's revelations and in part due to cybercriminals using Tor networks to protect their identities in online marketplaces as well as to control their bot network command centers. Also, the report notes that the majority of the new crimeware marketplaces opened in 2013 and later were hosted on "Deep Web" (wikipedia.org/wiki/Deep_Web) hosting servers accessible only by Tor browsers. Also, the report states that Bitcoin is now the de facto payment method in the majority of crimeware marketplaces. There are no statistics about the market share of the Deep Web hosted crimeware marketplaces with respect to all crimeware marketplaces, but these technologies are the preferred choice for new marketplaces as well as for any upgrades in the old crimeware marketplaces.

The anonymity of these technologies lowers the risk of conducting business in crimeware marketplaces, which possibly will increase the overall number of participants in cybercrime activities. In addition, the effect of these technologies goes beyond the cybercrime domain into other domain such as money laundering and cyberterrorism. Although e-currency money-laundering activities are still in their infancy, compared to regu-

Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

lar-currency money laundering, Bryans (2014) predicts an increase in e-currency money-laundering activities due to the lack of foresight by regulation writers, which creates a legal grey area. Thus, criminals can continue to capitalize on the unique features of e-currencies to grow their "businesses". Although Jarvis and colleagues (2014) concluded that cyberterrorism is still in an early stage, crimeware marketplaces coupled with anonymity technologies can lower the technical barrier required to launch such attacks, which may increase the risk of cyberterrorism in the near future.

Conclusion

Cybercrime activities are expected to continue to grow and their impact on the global economy will increase. In this article, we have identified three facilitating technologies in crimeware marketplaces that simultaneously offer anonymity and enable cybercriminals to reach an increasing number of targets. These technologies present new challenges to law enforcement agencies, governments, financial institutions, and corporations. More regulations are needed for e-currency exchanges to try to minimize their illegal use. Periodic monitoring and content analysis of crimeware marketplaces can enable the prediction of near-future small to mid-size security threats.

About the Author

Mahmoud M. Gad is a PhD candidate in Electrical and Computer Engineering with a focus on wireless network communications at the University of Ottawa in Canada. Additionally, he holds an MSc in Electrical and Computer Engineering from the University of Maryland in College Park, United States. His research interests include chaos-theory-based security algorithms for wireless networks, analysis of large-scale networks, Internet of Things (IoT), cognitive radio networks, and data mining algorithms.

References

Ablon, L., Libicki, M. C., & Golay, A. A. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Report number: RR-610-JNI.* Santa Monica, CA: RAND Publications. http://www.rand.org/pubs/research_reports/RR610.html

Atwal, R., Tay, L., Cozza, R., Nguyen, T. H., Tsai, T., Zimmermann, A., & Lu, C. K. 2013. *Forecast: PCs, Ultramobiles, and Mobile Phones, Worldwide, 2010-2017, 4Q13 Update.* Stamford, CT: Gartner. http://www.gartner.com/doc/2639615

Ben-Itzhak, Y. 2009. Organised Cybercrime and Payment Cards. *Card Technology Today*, 21(2): 10–11. http://dx.doi.org/10.1016/S0965-2590(09)70057-X

Bryans, D. 2014. Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal,* 89(1): 441-472. http://www.repository.law.indiana.edu/ilj/vol89/iss1/13

Caballero , J., Grier, C., Kreibich , C., & Paxson, V. 2011. Measuring Pay-Per-Install: The Commoditization of Malware Distribution. *Proceedings of the 20th USENIX conference on Security:* 13. San Francisco, CA: USENIX.

The Economist. 2014. The Amazons of the Dark Net. *The Economist,* November 1, 2014.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. 2007. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS) 2007.* Alexandria, VA: Association for Computing Machinery. http://dx.doi.org/10.1145/1315245.1315292

Fox-Brewster, T. 2014. Silk Road 2.0 Targeted in 'Operation Onymous' Dark-Web Takedown. *The Guardian,* November 7, 2014.

Goncharov, M. 2012. *Russian Underground 101.* Cupertino, CA: Trend Micro Incorporated.

Goncharov, M. 2014. *Russian Underground Revisited.* Cupertino, CA: Trend Micro Incorporated.

Gu, L. 2014. *The Mobile Cybercriminal Underground Market in China.* Cupertino, CA: Trend Micro Incorporated.

Holt, T. J. 2013. Examining the Forces Shaping Cybercrime Markets Online. *Journal Social Science Computer Review,* 31(2): 165-177. http://dx.doi.org/10.1177/0894439312452998

Internal Revenue Service. 2014. *IRS Notice 2014-21.* United States Internal Revenue Service. http://www.irs.gov/pub/irs-drop/n-14-21.pdf

Jarvis, L., Macdonald, S., & Nouri, L. 2014. The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism,* 37(1): 68-90. http://dx.doi.org/10.1080/1057610X.2014.853603

Jianwei, Z., Liang, G., & Haixin, D. 2012. *Investigating China's Online Underground Economy.* San Diego, CA: University of California Institute on Global Conflict and Cooperation.

Kshetri, N. 2010. *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives.* London: Springer. http://dx.doi.org/10.1007/978-3-642-11522-6

Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

Kowalski, M. 2002. *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.* Statistics Canada Catalogue No. 85-558-X. Statistics Canada, Canadian Centre for Justice Statistics.

Kraemer-Mbulaa, E., Tangb, P., & Rusha, H. 2013. The Cybercrime Ecosystem: Online Innovation in the Shadows? *Technological Forecasting and Social Change,* 80(3): 541–555. http://dx.doi.org/10.1016/j.techfore.2012.07.002

Lovet, G. 2006. Dirty Money on the Wires: The Business Models of Cybercriminal. Montreal: Virus Bulletin Conference 2006.

Lusthaus, J. 2013. How Organised is Organised Cybercrime? *Global Crime,* 14(1): 52–60. http://dx.doi.org/10.1080/17440572.2012.759508

McAfee. 2013. *The Economic Impact of Cybercrime and Cyber Espionage.* Center of Strategic and International Studies Report. Santa Clara, CA: McAfee.

McAfee. 2014. *Net Losses: Estimating the GlobalCost of Cybercrime.* Center for Strategic and International Studies. Santa Clara, CA: McAfee.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org.* November 1, 2014: http://bitcoin.org/bitcoin.pdf

Porter, M. E. 1985. Competitive Advantage: Creating and Sustaining Superior Performance. New York: The Free Press.

SERT. 2013. *Quarterly Threat Intelligence Report - Q3, 2013.* Omaha, NE: Solutionary Security Engineering Research Team (SERT).

Sherr, I., & Ovide, S. 2013. Computer Sales in Free Fall. *Wall Street Journal,* April 11, 2013.

Sod, A. K., & R. J. Enbody. 2013. Crimeware-as-a-Service: A Survey of Commoditized Crimeware in the Underground Market. *International Journal of Critical Infrastructure Protection,* 6(1): 28-38. http://dx.doi.org/10.1016/j.ijcip.2013.01.002

Symantec. 2008. *Symantec Report on the Underground Economy: July 07–June 08.* Mountain View, CA: Symantec Corporation.

Thomas, R., & Martin, J. 2006. The Underground Economy: Priceless. *Login,* 31(6): 7-16.

United States, Department of the Navy. 2014. BAA for CTTSO/TSWG Support. Solicitation Number: N41756-14-Q-3272.

Van Name, T. 2014. BitCoin Now on Bloomberg. Press release: April 30, 2014.

Yu, R. 2013. GinMaster: A Case Study in Android Malware. Berlin: Virus Bulletin Conference 2013.

Zetter, K. 2013. How the Feds Took Down the Silk Road Drug Wonderland. *Wired,* November 19, 2013.

Citation: Gad, M. 2014. Crimeware Marketplaces and Their Facilitating Technologies. *Technology Innovation Management Review*, 4(11): 28–33. http://timreview.ca/article/847

Keywords: cybercrime, dark web, underground economy, Bitcoin, anonymity, crimeware marketplaces

Assessing the Intentions and Timing of Malware

Brent Maheux

"*Bien mal acquis ne profite jamais.*"

(Ill-gotten gains seldom prosper.)

French proverb

Malware has become a significant, complex, and widespread problem within the computer industry. It represents one of the most prevalent threats to cybersecurity and is increasingly able to circumvent current detection and mitigation techniques. To help better understand when a malware attack might happen, this article proposes an intention-based classification of malware and merges it with an optimal timing model to help predict the timing of malware based on its classification. The classification model is based on an examination of eight malware samples, and it identifies four malware classifications and commonalities based on the dimensions of persistence and stealth. The goal of the article is to provide a better understanding of when cyber-conflict will happen, and to help defenders better mitigate the potential damage.

Introduction

In today's online environment, computer systems now dominate our personal, business, and financial lives. However, our dependency on these systems also makes us vulnerable to cybercriminals. The cost of cybercrime now exceeds $110 billion USD and affects 566 million victims annually, which equates to 1.5 million victims per day or 18 victims per second (Semantec, 2012). Malware, which is short for "malicious software" and includes computer viruses, worms, trojan horses, and spyware (TechTerms, 2014), which are used for a range of illicit activities such as distributing spam email and stealing sensitive information.

Although there has been a lot of research on detecting malware (e.g., Baecher et al., 2006; Gu et al., 2007; Invernizzi et al., 2014; Jain & Bajaj, 2014; Jiang et al., 2007; Peng et al., 2013) and analyzing it from a technical perspective (e.g., Dinaburg et al., 2008; Jain & Bajaj, 2014; Moser et al., 2007; Willems et al., 2007; Yin et al., 2007), there is a lack of research on timing and categorizing malware based on its intentions. A greater understanding of the intentions of attackers will increase the defender's knowledge on how to mitigate attacks.

This article examines an evolutionary timeline of malware based on eight examples of malware dating from the first computer virus in 1971 (Gatto, 2011) through to a recent example from 2012. These examples are used to develop an intention-based classification of malware, which is then combined with Axelrod and Iliev's (2013) optimal timing model. The optimal timing model deals with the question of when the malware should be used given that its use today may well prevent it from being available for use later. The optimal timing model is presented from the perspective of the offense – helping predict the best time to use a resource. However, the results are equally relevant to a defender who wants to estimate how high the stakes have to be in order for the offense to use their resource. When the optimal timing model is combined with the intention-based classification, the new model helps clarify how the timing of malware can depend on the stakes involved in the present situation, as well as the characteristics of the resource for exploitation. Even further, the model helps predict the level of sophistication one could be facing, increasing the chances of mitigating the malware (Galarneau, 2002; Mell et al., 2005; Symantec, 2014).

Axelrod and Iliev test their optimal timing model on four individual case study examples. Combining the model on a broader class of malware samples will further test their model or allow new perspectives and theories to evolve. Because both models use the same definitions for a malware's stealth and persistence capabilities, they can be easily combined to provide a better understanding of the intentions and timing of the attacker's malware.

Assessing the Intentions and Timing of Malware

Brent Maheux

This article is structured as follows. The first section describes and analyzes eight examples of malware, from the first computer virus in 1971 to a case of cyberwarfare in 2012. Next, Axelrod and Iliev's (2013) optimal timing model is introduced and applied to the context of malware. Then, drawing upon the examples of malware analyzed earlier, an intention-based classification of malware is proposed and combined with the optimal timing model to illustrate how the optimal timing of malware can be determined depending on the attacker's intentions. The final section provides conclusions.

Examples of Malware

In this section, eight examples illustrate the evolution of malware, ranging from the first experimental computer virus from 1971 to a cyberespionage application that was discovered in 2012. These eight cases were selected as being noteworthy examples of malware based on a combination of timelines (Hansen, 2013; Infoplease, 2012; Khanse, 2014; Larsen, 2012; Malware Database, 2014; PC History, 2003; Standler, 2008). The eight examples are spread out over the history of malware and are generally representative of contemporary malware examples.

1. *Creeper:* The first virus. In 1971, the Creeper system, now considered to be the first computer virus, was an experimental self-replicating program that infected DEC PDP-10 computers running the TENEX operating system (Gatto, 2011). Creeper gained access via the ARPANET by searching for a machine within the network, transferring itself, displaying a message, then starting over, thereby hopping from system to system. It was developed for experimental purposes, as a proof of concept within an academic research context.

2. *Elk Cloner:* The first outbreak. Elk Cloner was created in 1982 as a prank by a 15-year-old high school student. The virus attached itself to the operating system of Apple II computers and then spread itself via floppy disk to other computers, on which it would display a poem instead of loading a game. Elk Cloner is one of the first known viruses that spread beyond the computer system or laboratory in which it was written (Rouse, 2005).

3. *Happy99:* The happy worm. As the name suggests, this worm was developed 1999 and usually arrived as an email attachment or new post that was named Happy99.exe. Once executed, Happy99 would display fireworks, then copy itself to the windows system folder and then email itself to all contacts listed on the system. Lacking any destructive payload, Happy99 would not cause damage to the actual affected computer; it was simply a prank (Elnitiarta, 2007).

4. *Code Red:* Vulnerable web servers. In 2001, Code Red infected web servers, where it automatically spread by exploiting a known vulnerability in Microsoft IIS servers. In less than one week, nearly 400,000 servers were infected, and the homepage of their hosted websites was replaced with the message "Hacked By Chinese!" Code Red had a distinguishing feature designed to flood the White House website with traffic from the infected servers, which likely makes it the first case of documented political "hacktivism" on a large scale (Lovet, 2011).

5. *Blaster:* A large prank. In 2003, the Blaster worm spread on computers running the Microsoft operating systems Windows XP and Windows 2000, with damage totaling in the hundreds of millions (Dougherty et al, 2003). It was notable for the two hidden text strings, the first of which said "I just want to say LOVE YOU SAN!" and the second of which was a message to Microsoft CEO Bill Gates.

6. *Zeus:* Malware as a service. Over $70 million USD was stolen from users who were infected with the Zeus malware. It was one of the first major botnet malware applications that would go undetected by updated antivirus and go unnoticed by people who were using infected computers. Zeus was capable of being used to carry out malicious and criminal tasks, often being used to steal banking information. Zeus initially started to infect computers in 2007, and by 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as Bank of America, NASA, Monster.com, ABC, Oracle, Cisco, Amazon, and BusinessWeek (Ragan, 2009).

7. *Stuxnet:* The stealthy one. Discovered in 2010, the Stuxnet virus would propagate across a network, scanning for unique Programmable Logic Controllers (PLCs) and certain software. Once it found the correct machine to reside on, it would infect the machine with a rootkit and start modifying the code, giving unexpected commands to the PLC while returning a loop of normal operating system values to the users. Multiple zero-day exploits were used on an estimated 16,000 computers that were infected by the Stuxnet virus, including Iran's nuclear enrichment plant at Natanz (Emerson, 2012).

Assessing the Intentions and Timing of Malware

Brent Maheux

8. *Flame:* Cyberespionage. Flame is a modular computer malware application discovered in 2012 that attacks computers running the Microsoft Windows operating system. The program is being used for targeted cyberespionage in Middle Eastern countries. Flame can spread over systems through the local area network (LAN) or via USB device and has the ability to record audio, screenshots, keyboard activity, and network traffic. According to estimates by Kaspersky in May 2012, Flame had initially infected approximately 1,000 machines with victims including governmental organizations, educational institutions, and private individuals. In total, Kaspersky estimates more than 5,000 computers were infected (Kaspersky Lab, 2013).

As shown in Table 1, the eight examples of malware can be summarized along the following six dimensions:

1. *Year:* date of first discovery.

2. *Intention:* the reason the malware was created. Types of intentions include experimental (including research, entertainment, demonstrations of skill), financial (including theft and fraud), political (including "hacktivists"), and cyberwarfare (including state-sponsored attacks).

3. *Initial access:* how the malware gained access to the system or network. Means of initial access include social engineering (i.e., psychological manipulation), a zero-day vulnerability (i.e., a previously unknown vulnerability in a computer application), and a known vulnerability.

4. *Stealth:* the probability that, if you use a resource now, it will still be available to use later (Axlerod & Iliev, 2013).

5. *Persistence:* the probability that, if you refrain from using a resource now, it will still be available to use in the future (Axlerod & Iliev, 2013).

6. *Extent:* the number of computers affected.

As Table 1 shows, the number of computers affected by the malware increases over time, except in the recent case of Flame, which is malware for targeted espionage, not widespread impact. Early examples of malware were readily detected and did not persist for long, and tended to rely on known vulnerabilities and social engineering for initial access. Later examples, particularly in malware for cyberwarfare, show a trend toward more targeted attacks with increased stealth and persistence.

Modelling Malware Based on Intentions and Timing

The design and features of a particular malware application will depends on the creator's intentions, and its users must also take into account the optimal timing of its desired impact. In the general context of cybersecur-

Table 1. Examples of malware

Name	Year	Intention	Initial access	Stealth	Persistence	Extent
Creeper	1971	Experimental	Known vulnerability	Low	Low	< 1k
Elk Cloner	1982	Experimental	Social engineering	Low	Low	< 1k
Happy99	1999	Experimental	Social engineering	Low	Low	10k
Code Red	2001	Political	Known vulnerability	Medium	High	400k
Blaster	2003	Experimental	Known vulnerability	Low	Low	8M
Zeus	2007	Financial	Social engineering	Medium	Low	3.6M
Stuxnet	2010	Cyberwarfare	Zero-day	High	High	16k
Flame	2013	Cyberwarfare	Zero-day	High	High	1k

Assessing the Intentions and Timing of Malware

Brent Maheux

ity, Axelrod and Iliev (2013) developed an optimal timing model to help understand when a given attacker should exploit its capacity to do harm. Their model considers important assumptions about the stakes at hand and the resource characteristics in terms of stealth and persistence:

1. *Stakes:* their model assumes that the attacker knows the current stakes of how important the target currently is but does not know what the stakes will be at any future point – although they do know the distribution of stakes over time.

2. *Stealth:* the probability that, if you use a resource now, it will still be available to use later.

3. *Persistence:* the probability that, if you refrain from using a resource now, it will still be available to use in the future.

Thus, Axelrod and Iliev's (2013) optimal timing model can be used to predict the optimal time to maximize the value of a particular malware application if an attacker knows the current stakes and the application's capabilities in terms stealth and persistence. An attack-value threshold can be calculated based on the malware's stealth and persistence and the capacity and vigilance of the intended target. For instance, the stealth of malware used against a well-protected target is likely to be less than the stealth of the same malware against a target that is not particularly attentive to security. Likewise, malware will typically have less persistence against a target that keeps its systems up-to-date with security patches than against a target that does not.

Thus, stealth and persistence depend on both the characteristics of the malware itself and the context of its use. Ideally, the attacker would have security knowledge of the systems they are trying to compromise. In the real world, and in Axelrod and Iliev's (2013) optimal timing model, the characteristics of stealth, persistence, and stakes can be weighted differently. However, for simplicity in this preliminary proposal, the model weighs each of the characteristics the same.

Overall, the optimal timing model predicts the three factors that favour attacker patience: low stealth, high persistence, and low stakes. However, when the stakes are high, the model favours high stealth and low persistence. Indeed, based on the analysis of the cases shown in Table 1, the attacker's intentions can be mapped along the two dimensions of stealth and persistence, as shown in Figure 1.

The political malware examples would be found in the top left corner of Figure 1, which is characterized by high persistence and low stealth. For example, "hacktivist" malware often has high persistence and goes undetected until the group wants to raise awareness of a particular situation (Tarzey & Fernandes, 2013). Cyberwarefare malware uses high stealth and high persistence to stay undetected for as long as possible. Financial malware has high stealth, enabling its creators to steal information through social engineering or misleading users; however, it has low persistence because cases of social engineering often have a limited lifespan because they are often based on current events (Conheady, 2012). The final classification is experimental, with low stealth and low persistence, experimental malware does not persist on computers nor does have a potential lifespan because they are often based off of publicly known weaknesses in a system and are created simply to show how an attacker can take advantage of the weakness. Within the set of malware samples studied in this article, all experimental malware displayed messages indicating that it was on the computer and then it would be deleted by users or the vulnerability would be patched.

The classification shown in Figure 1 can be enhanced by introducing variable stakes, as described in Axelrod and Iliev's (2013) model. Table 2 shows three scenarios of low, constant, and high stakes and the optimal timing for the use of malware depending on its intention. When the stakes are low, the optimal timing model determines that the current time is not the optimal time to use the malware for any malware classification, except, potentially financial malware.

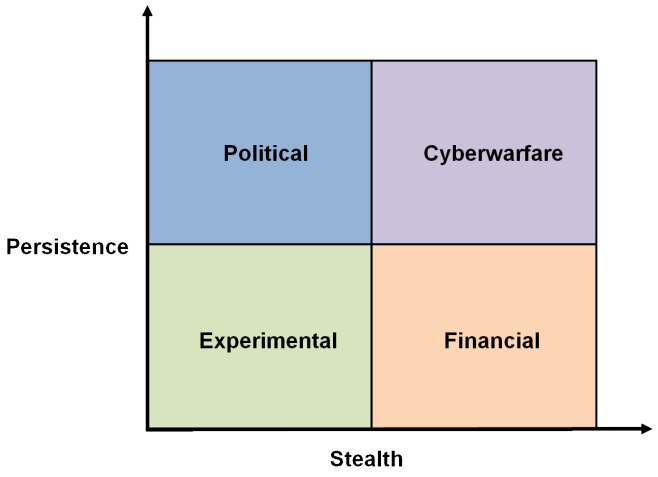

Figure 1. An intention-based classification of malware

Assessing the Intentions and Timing of Malware

Brent Maheux

Under constant stakes, the results in Table 2 show that financial malware should be used immediately. The model suggests the use of financial malware because, as defined by the intention-based classification, financial malware has low persistence and high stealth, making it the exact candidate to use under the optimal timing model. For example, a setting where the stakes are constant over time is the exploitation of stolen credit card information.

Under high stakes, the results in Table 2 show that it is optimal to use the resource immediately, except perhaps when the intention is political. The famous political, or "hacktivist" group, Anonymous, continues to use their resources, but only to send a message relating to a particular event. There is likelihood that they believe their message should be voiced on a particular world event so their stakes are so large that they are willing to sacrifice their resources to do so.

It is important to note the limitations of these results using the same weight for each of the three variables: persistence, stealth, and stakes. In real world examples, and in Axelrod and Iliev's optimal timing model, these values can be weighted differently.

Conclusion

It has been more than 40 years since our first example of malware. Malware evolved, but some of the principles have remained the same. The purposes and motives for malware have changed from educational, protests, and pranks to profit then finally to espionage and sabotage. Intention is an important part of understanding malware; originally, antivirus companies were looking for malware that had financial profit, so many systems were being skipped. Knowing that malware is also being used by governments and military, the search for potential malware activities can be broadened to other poten-

Table 2. The optimal timing of malware use depending on intentions, persistence, stealth, and stakes

Low Stakes	**Intention**	**Persistence**	**Stealth**	**Timing**
	Political	High	Low	Wait
	Cyberwarfare	High	High	Wait
	Experimental	Low	Low	Wait
	Financial	Low	High	---
Constant Stakes	**Intention**	**Persistence**	**Stealth**	**Timing**
	Political	High	Low	Wait
	Cyberwarfare	High	High	---
	Experimental	Low	Low	---
	Financial	Low	High	Use now
High Stakes	**Intention**	**Persistence**	**Stealth**	**Timing**
	Political	High	Low	---
	Cyberwarfare	High	High	Use now
	Experimental	Low	Low	Use now
	Financial	Low	High	Use now

Assessing the Intentions and Timing of Malware

Brent Maheux

tial systems. Understanding the intentions of malware enables the evaluation of the effectiveness of malware defenses.

The concept of initial access has changed slightly over the years. Many of the early examples of malware discussed here needed to be distributed, for instance through email, floppy disk, or USB device, or through a vulnerability in a web service that has an open port. However, the more recent examples – Stuxnet and Flame – were using zero-day exploits. This pattern may be a relatively new trend, because organizations are no longer telling the public or the vulnerable vendors about vulnerabilities; instead they are keeping or selling the techniques (Radianti & Gonzalex, 2007). Again, understanding the purpose of the malware helps in determining how many systems might be affected and how they originally became compromised. If the purpose is financial gain, then it seems likely that many systems will be infected. However, for cyberwarfare, or government-related instances, the examples studied show that only a small, unique set of systems will be infected.

Presented in this article is a model that represents the majority of malware today. The model was created to help understand the potential effectiveness of a malware application's stealth and persistence techniques based on their intentions. And, by combing the optimal timing model by Axelrod and Iliev (2013) with the results of studying the eight malware samples, Table 2 can help predict when an initial attack would likely happen.

About the Author

Brent Maheux is a Senior Software Specialist for the Canadian Government. He holds an MEng degree in Technology Innovation Management from Carleton University in Ottawa, Canada, and a BCS degree in Computer Science from Dalhousie University in Halifax, Canada. He has over 7 years working experience within the public and private sector specializing in product design and implementation.

References

Axelrod, R., & Iliev, R. 2013. Timing of Cyber Conflict. *Proceedings of the National Academy of Sciences of the United States of America,* 111(4): 1298-1303. http://dx.doi.org/10.1073/pnas.1322638111

Baecher, P., Koetter, M., Holz, T., Dornseif, M., & Freiling, F. 2006. The Nepenthes Platform: An Efficient Approach to Collect Malware. *Recent Advances in Intrusion Detection,* 4219: 165-184. http://dx.doi.org/10.1007/11856214_9

Conheady, S. 2012. The Future of Social Engineering. *Privacy PC.* July 17, 2012. http://privacy-pc.com/articles/the-future-of-social-engineering.html

Dinaburg, A., Royal, P., Sharif, M., & Lee, W. 2008. Ether: Malware Analysis Via Hardware Virtualization Extensions. *Proceedings of the 15th ACM Conference on Computer and Communications Security:* 51-62. http://dx.doi.org/10.1145/1455770.1455779

Dougherty, C., Havrilla, J., Hernan, S., & Lindner, M. 2003. W32/Blaster Worm. Historical Advisory CA-2003-20, CERT Division of the Software Engineering Institute. October 1, 2014: http://www.cert.org/historical/advisories/CA-2003-20.cfm

Elnitiarta, R. 2007. Security Response: Happy99.Worm. *Symantec.* October 1, 2014: http://www.symantec.com/security_response/writeup.jsp?docid=2000-121812-3151-99

Emerson, R. 2012. Stuxnet Virus Infected 16,000 Computers, Iran Says. *Huffington Post*, February 18, 2012: http://www.huffingtonpost.com/2012/02/18/stuxnet-virus-iran_n_1286281.html

Galarneau, L. 2002. Anti-virus Software: The Challenge of Being Prepared for Tomorrow's MalWare Today. SANS Institute 2002.

Gatto, K. 2011. The Virus Turns 40. *Phys Org.* November 1, 2014: http://phys.org/news/2011-03-virus.html

Gruener, W. 2012. Kaspersky: Flame Has Three Unidentified Malware Siblings. *Tom's Hardware.* November 1, 2014: http://www.tomshardware.com/news/virus-flame-stuxnet,17644.html

Gu, G., Porras, P., Yegneswaran, V., Fong, M., & Lee, W. 2007. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. *Proceedings of the 16th USENIX Security Symposium:* 167-182.

Hansen, P. 2013. History of Malware. *Technology Bell.* November 1, 2014: http://www.technologybell.com/history-of-malware/

Infoplease. 2012. Computer Virus Timeline. *Information Please.* November 1, 2014: http://www.infoplease.com/ipa/A0872842.html

Invernizzi, L., Miskovic, S., Torres, R., Saha, S., Lee, S., Mellia, M. Kruegel, C., & Vigna, G. 2014. Nazca: Detecting Malware Distribution in Large-Scale Networks. Network and Distributed System Security (NDSS) Symposium 2014. February 23, 2014.

Assessing the Intentions and Timing of Malware

Brent Maheux

Jain, M., & Bajaj, P. 2014. Techniques in Detection and Analyzing Malware Executables: A Review. *International Journal of Computer Science and Mobile Computing,* May, 2014 (5): 930–935.

Jiang, X., Wang, X., & Xu, D. 2007. Stealthy Malware Detection through VMM-Based "Out-of-the-Box" Semantic View Reconstruction. *Proceedings of the 14th ACM Conference on Computer and Communications Security:* 128-138. http://dx.doi.org/10.1145/1315245.1315262

Khanse, A. 2014. Evolution of Malware – How It All Began! *The Windows Club*. November 1, 2014: http://www.thewindowsclub.com/evolution-of-malware-virus

Kaspersky Lab, 2013. Who's Spying on You? *Kaspersky Lab*. November 1, 2014: http://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf

Larsen, C. 2012. A Malware Hall of Fame. *Blue Coat*. November 1, 2014: http://www.bluecoat.com/security/security-archive/2012-10-31/malware-hall-fame

Lovet, G. 2011. 40th Anniversary of the Computer Virus. *Help Net Security*. October 1, 2014: http://www.net-security.org/malware_news.php?id=1668

Malware Database. 2014. Timeline of Noteworthy Computer Viruses, Worms and Trojan Horses. *The Malware Database*. November 1, 2014. http://malware.wikia.com/wiki/Timeline_of_noteworthy_computer_viruses,_worms_and_Trojan_horses.

McDowell, M. 2013. Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks. *United States Computer Emergency Readiness Team*. November 1, 2014: https://www.us-cert.gov/ncas/tips/ST04-014

Mell, P., Kent, K., & Nusbaum, J. 2005. *Special Publication 800-83: Guide to Malware Incident Prevention and Handling.* Gaithersburg, MD: Nation Institute of Standards and Technology.

Moser, A., Kruegel, C., & Kirda, E. 2007. Exploring Multiple Execution Paths for Malware Analysis. *Proceedings of 2007 IEEE Symposium on Security and Privacy:* 231-245. http://dx.doi.org/10.1109/SP.2007.17

PC History. 2003. The History of the PC Virus. *PC History*. November 1, 2014: http://www.pc-history.org/pc-virus.htm

Peng, W., Li, F., Zou, X., & Wu, J. 2013. Behavioral Malware Detection in Delay Tolerant Networks. *IEEE Transactions on Parallel and Distributed Systems,* 25(1): 53–63. http://dx.doi.org/10.1109/TPDS.2013.27

Ragan, S. 2009. ZBot Data Dump Discovered with over 74,000 FTP Credentials. *The Tech Herald*. November 1, 2014: http://www.thetechherald.com/articles/ZBot-data-dump-discovered-with-over-74-000-FTP-credentials/6514/

Rouse, M. 2005. Elk Cloner. *SearchSecurity.com*. October 1, 2014: http://searchsecurity.techtarget.com/definition/Elk-Cloner

Semantec. 2012. 2012 Norton Cybercrime Report. Mountain View, CA: Symantec Corporation.

Semantec. 2014. *Preparing for Future Attacks*. Mountain View, CA: Symantec Corporation.

Standler, R. 2008. Examples of Malicious Computer Programs. *Website of Dr. Ronald B. Standler*. November 1, 2014: http://www.rbs2.com/cvirus.htm

Tarzey, B., & Fernandes, L. 2013. The Trouble Heading for Your Business. *Quocirca,* February 2013

TechTerms. 2014. Malware. *TechTerms.com*. November 1, 2014: http://www.techterms.com/definition/malware

Willems, C., Holz, T., & Freiling, F. 2007. Toward Automated Dynamic Malware Analysis Using CWSandbox. *IEEE Security & Privacy,* 5(2): 32-39. http://dx.doi.org/10.1109/MSP.2007.45

Yin, H., Song, D., Egele, M., Kruegel, C., & Kirda, E. 2007. Panorama: Capturing System-Wide Information Flow for Malware Detection and Analysis. *Proceedings of the 14th ACM Conference on Computer and Communications Security:* 116-127. http://dx.doi.org/10.1145/1315245.1315261

Citation: Maheux. B. 2014. Assessing the Intentions and Timing of Malware. *Technology Innovation Management Review,* 4(11): 34–40. http://timreview.ca/article/848

Keywords: malware, cybersecurity, optimal timing, stealth, persistence

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl,
Paul Soble, and D'Arcy Walsh

> *"The errors of a theory are rarely found in what it asserts explicitly; they hide in what it ignores or tacitly assumes."*
>
> Daniel Kahneman
> Nobel Laureate in Economic Sciences (2002)

In this article, we address what it means to be safe in the online world of the future by advocating the perspective whereby improving safety will improve resilience in cyberspace. We adopt a specific approach towards transdisciplinarity; present a weakly transdisciplinary model of the safety context and an initial position about what existing disciplines are most relevant; and link prospect theory to risk-based decision making as one example that could lead to a new paradigm for safety. By treating safety as a transdisciplinary challenge, there is an opportunity to enable the participants of the online world to become more productive and creative than ever before. The beneficiary of this increased productivity and creativity will ultimately be the public. The perspective of this article is of interest to senior decision makers, policy makers, managers, educators, strategists, futurists, scientists, technologists, and others interested in shaping the online world of the future.

Introduction

This article focuses on the nature of safety in the future online world to enable humanity to reach profoundly new levels of productivity and creativity. Bailetti, Levesque, and Walsh (2014) envision an online world for 2030 that is safe (i.e., users communicate with accuracy and enduring confidence), productive (i.e., users make timely decisions that have an ongoing global effect), and creative (i.e., users can connect seemingly unrelated information online). Their proposed view is characterized by seven conditions of the future online world: i) global-scale autonomous learning systems; ii) humans co-working with machines; iii) human factors that are authentic and transferrable; iv) global scale whole-brain communities; v) foundational knowledge that is authentic and transferrable; vi) timely productive communication; and vii) continuous technological adaptation.

Key research questions pertaining to the safety characteristics of this future world include:

- Under what conditions does an attacker have an advantage over an infrastructure protector?
- Why do many infrastructure protectors and users not adopt effective mechanisms that provide safety and privacy?
- What are the resources, processes, and values to concurrently provide online safety and privacy to users?
- What are the characteristics of the individuals and organizations that are most likely to attack?
- What are the enhanced characteristics of safety through disclosure (i.e., by being open and not by being proprietary)?

If progress is made understanding the underlying properties of safety that are required to address these questions, then a foundation will be provided that promotes scientific progress and the arts within a society that is ever more connected on a global scale.

The Internet was not created to be safe but is being increasingly used in a way that requires that it be so. The increasing pervasiveness of cyber-based systems and infrastructure, and society's growing reliance on them, shifts the perspective concerning their proper opera-

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

tion from security to safety. Although defending networks and other information assets is necessary, it is part of the larger intent of securing these systems' ability to produce services and functions upon which society depends. Safety is often associated with unintended disruption, and security is often associated with intended disruption; both concepts affect the proper operation of cyber-based systems and infrastructure. Safety properties include security properties (Burns et al., 1992; Leveson, 2013; Young & Leveson, 2013). Safety is the foundation that promotes scientific progress and the arts within a society that is ever more connected on a global scale; it enables the global knowledge commons that is an engine of human progress.

This view of safety is sympathetic and compatible with the ultimate intent of copyright and patent laws. Article I of the American Constitution makes clear that the beneficiary of publications and inventions is the public – copyrights are granted and patents are issued in order "to promote the Progress of Science and useful Arts" (Menard, 2014). The thinking behind Article I is that prohibiting people from copying and selling someone else's original work should be time bound to strike an appropriate balance so that individuals and organizations have the means to further create original work but in a manner that the public can also benefit from this work in a timely fashion (Menard, 2014).

In this spirit, the concept of safety (including security) is not restricted to the protection and control of property, because ownership is a concept that can vary across social contexts. Instead, improving the safety of cyber-based systems and services focuses on the intended use of these systems. Further, safety must have enduring resilience where "cyber- [or online] resilience is about digital literacy at every level of the organization/society, distributed leadership, and a capacity to adapt in a networked and fast-changing digital ecosystem" (Rütten, 2010). Thus, there is a responsibility for safety that transcends the technological disciplines.

Based upon our knowledge and experience, current approaches toward safety and security do not make an explicit connection to productivity and creativity when contemplating the transdisciplinary aspects of the problem domain. These approaches emphasize preventing failure instead of enabling success. A new online paradigm that implies an environment that is safe regardless of how much you interact within it is necessary "to promote the Progress of Science and useful Arts" (Menard, 2014) in the future.

This article makes three contributions. First, it provides insight about a particular approach for addressing the global and transdisciplinary aspects that we believe characterize safety concerns of the online world of the future. Second, the article presents a weak transdisciplinary representation of the safety context and an initial position about what existing disciplines are most relevant. Third, by linking prospect theory to risk-based decision making within the domain of cyber-resilience, it provides an example to advance the idea of safety through online interactivity that could lead to a new paradigm for safety for the future online world.

The Safety Context is Global and Transdisciplinary

A safe online world must be created and maintained by stakeholders at multiple levels of society, which suggests that a more holistic view is required to define goals and engage participants rather than following separate approaches to the problem from distinct disciplines, which individually tend to address a subset of stakeholders. The concerns of these stakeholders are accommodated by treating relevant disciplines in a unified way. The concept of transdisciplinarity (Nicolescu, 2005), creating a unity of intellectual frameworks beyond the disciplinary perspectives (Jensenius, 2012), offers an approach for constructing a view of safety as a composition of collaborating disciplines that address the concerns of these stakeholders.

A distinction may be made between strong and weak transdisciplinarity. Strong transdisciplinarity envisions a total system of knowledge without stable boundaries between the disciplines. However, in the case of weak transdisciplinarity, traditional methods and logic can be applied. Here, we focus on weak transdisciplinarity, where a transdiscipline extends its action through coordination among disciplines at several levels of organization: the first, lowest level refers to "what exists now" (i.e., the world as it is; the empirical level), the second level refers to "what we are capable of doing" (i.e., it is composed mainly of technology disciplines; the capacity level), the third level refers to "what we want to do" (i.e., the normative level), and the fourth level refers to "what we should do" (i.e., the value level) (Max-Neef, 2005).

Thus, we do not treat safety as strictly disciplinary (specialization in isolation), multidisciplinary (no cooperation), pluridisciplinary (cooperation without coordination), or interdisciplinary (coordination from a higher-level concept), but instead we treat it as a coordination amongst all hierarchical levels.

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

In an effort to practice weak transdisciplinarity in a systematic manner as advocated by Max-Neef (2005), we have adopted a four-level organization model at the core of the safety context, and a set of high-level categories of knowledge that should be coordinated to achieve a safe online environment (Figure 1):

1. *Online world of the future:* speculates about the safe, productive, creative aspects that will drive the evolution of the online world, including the key conditions that will be met by the future world (see Bailetti et al., 2014).

2. S*trategy for making scientific progress and transfer of knowledge:* includes research questions, research methods and techniques, new disciplines, assessment of progress, and the transfer of knowledge through education and other means.

3. *Legal/ethical concerns:* includes issues related to privacy, security, intellectual property, regulation, disclosure, and human-machine interaction for the individual and collective good.

4. *Human sciences:* includes human behaviour, cognition, and social dynamics; how people think, how people interact, and how societies and groups behave; what people think, their beliefs and ideologies; cultural factors; and value systems.

5. *Technical understanding of the communication environment:* includes issues related to scientific understanding and technical aspects, including real-time, manifestation of phenomena within the online environment and the deployment of interconnected systems of systems.

6. *Related domain models:* concern the promotion of specific theories or concepts relevant to the domain, for example: the Cyber Game (information versus power); safety (unintended and intended disruption); economic models (public, private, club, common pooled resource); political science models; human behavior (decision making under risk, deception, intent); technical methods and techniques related to attack, attribution, forensics, and impact of compromise; and specific business models.

7. *Important topics:* include specific perspectives or "game changers" that represent current informed thinking about the domain (e.g., supply/value chain; duality of risk – opportunities, threats; adoption; disclosure, disruption).

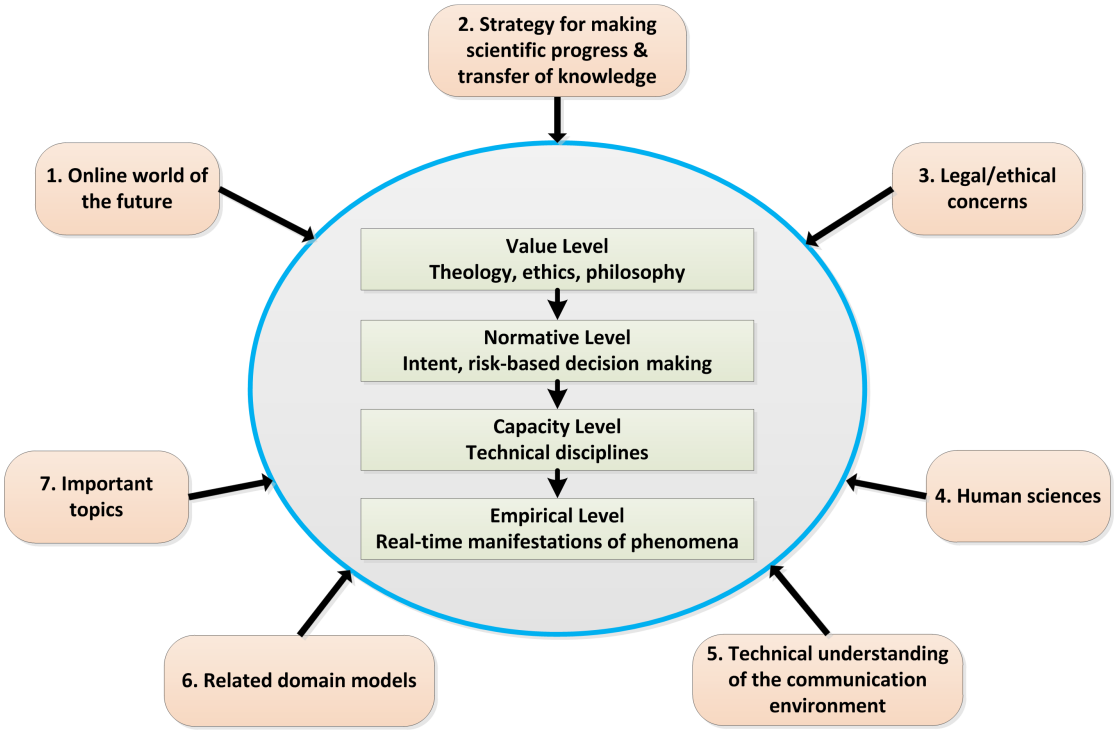

Figure 1. Four levels of concerns that need to be addressed to produce a safe online environment and seven categories of knowledge that influences the work done on these concerns.

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

Specific to the domain, we believe that the "Cyber Game" from the Global Cyber Game report (Tibbs, 2013) presents a useful domain analysis of the online world. The report was produced by the United Kingdom's Defence Academy, which provides education and training in a broad range of subjects – including command and staff, leadership, defence management, languages, acquisition and technology – for members of the UK Armed Forces and Defence Civil Servants. In delivering education and training, it is the Defence Academy's responsibility to prepare senior decision makers for the uncertainties and complexities of the challenges ahead. The report is a good example of this preparation as it pertains to the nature of cyberspace in the future, including cybersafety and cybersecurity.

The overall objective when producing the report was first to consider the broad question, "How should the cyber-domain be conceptualized?", and in the light of that question, to examine the implications for security strategy generally, the issues raised for state actors in the Internet age, new power relationships, possible sources and modes of future conflict, and the steps that need to be taken to prepare for a range of plausible possibilities (Tibbs, 2013).

The report examines these issues, in part, by proposing the idea of the Global Cyber Game as a framework that can be used for practical thinking about cyber strategy. Cyberpower and cybersecurity are conceptualized using a "Cyber Gameboard", which consists of a nine-cell grid. The horizontal direction on the grid is divided into three columns representing aspects of cyber-information: connection, computation, and cognition. The vertical direction on the grid is divided into three rows representing types of power: coercion, co-option, and cooperation. The nine cells of the grid represent all the possible combinations of power and information, that is, forms of cyberpower (Tibbs, 2013).

The central ideological decision of the Cyber Game is whether to play the game as if freedom of information content is a public good in itself or whether extensive control of information content is necessary for public safety (Tibbs, 2013).

Thus, the Cyber Game gives precedence to the concepts of information and power and the interrelationships that can arise when these two concepts are applied together. The Cyber Gameboard is a concise but powerful representation that permits reasoning about many of the aspects and complex interactions of cyberspace to achieve an outcome that can be successful despite, for example, known ideological conflicts, politics, and human nature whose complexity requires coordinated action.

The power dimension of the Cyber Game privileges the sub-concepts of cooperation (integrative social power), co-option (economic exchange power), and coercion (destructive hard power) as means to exercise power. On this dimension, cyberspace is a tool similar to new technologies such as airpower or net-centric warfare used to achieve effects on geopolitical actors with its own characteristics of power transition versus power diffusion.

The information dimension of the Cyber Game privileges the sub-concepts of connection (the physical data-handling domain), computation (the virtual interactivity domain), and cognition (the knowledge and meaning domain). On this dimension, an example bridging the gap from cyberspace to physical space is the Stuxnet case study of a cyber attack strategy to bridge connection, computation and cognition spaces (Kushner, 2013).

A Weak Transdisciplinary Representation of the Safety Context

This section introduces a weak transdisciplinary representation of the safety context of cyberspace and an initial position about what existing disciplines are most relevant. Because we lack a methodology for applying weak transdisciplinarity, our approach is based on our subjective confidence.

Figure 2 presents Cyber Game concepts and related disciplines using the four-level organizational model, including connections that cascade from the Value Level, through the Normative and Capacity Levels, to the Empirical level to indicate the coordination that must happen across levels amongst those concepts that are linked. Although the structure does not directly answer questions such as "What does it mean to be safe?" or "Who is safe from whom or what?", it unifies the elements that must be adjusted to evolve from the present situation toward the preferable future (Bailetti et al., 2014) in a way that addresses the multi-level complexity of the problem.

What we should do is addressed at the Value Level of Figure 2, including theology, values, security and privacy, intellectual property, regulation, disclosure, and the individual and collective good as they relate to human–machine interaction. Practical solutions must in-

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

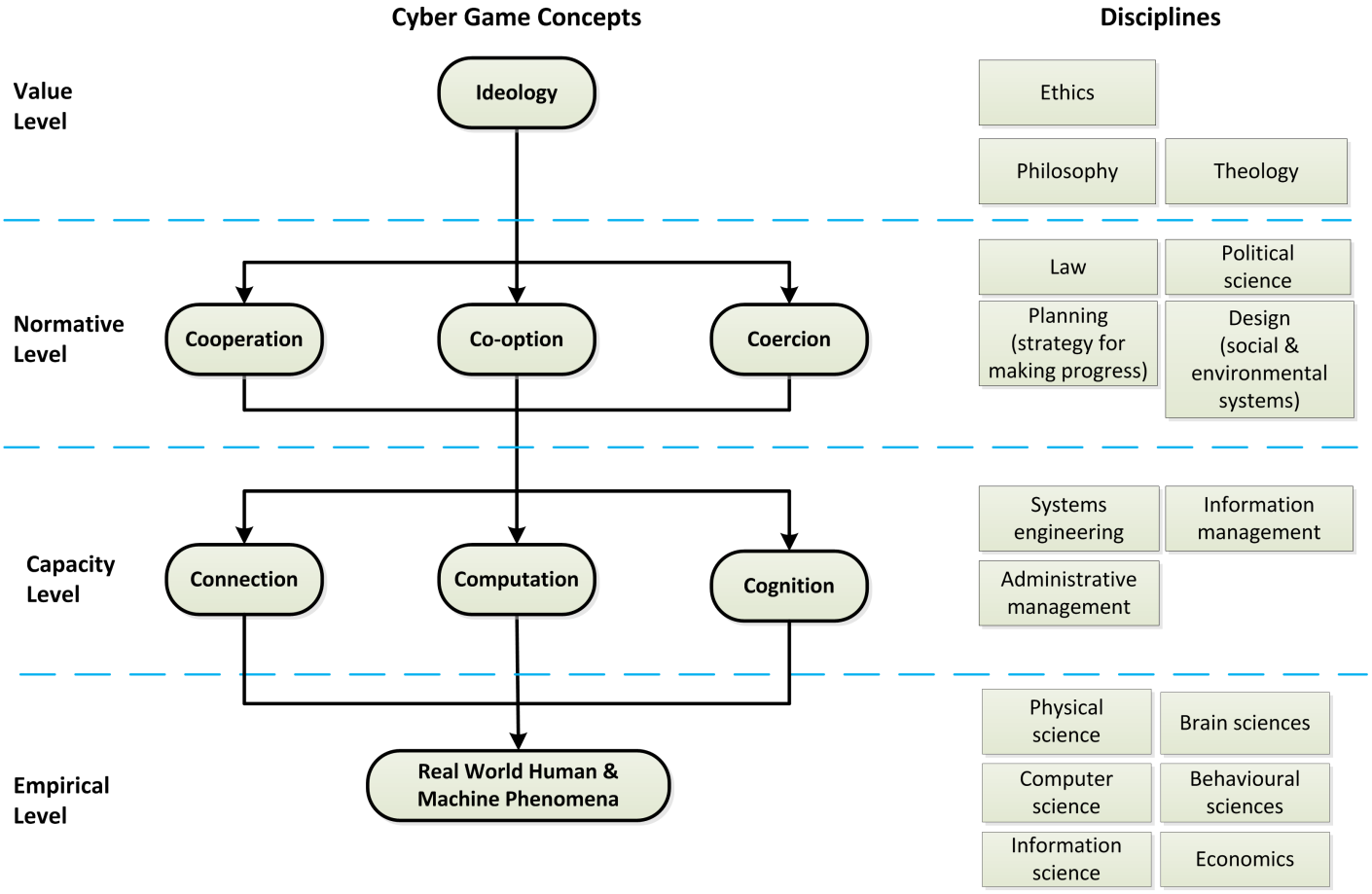

Figure 2. Cyber Game concepts and related disciplines categorized using the four-level model

volve this level to account for online participants who do not share the same views of such things as values, religion, and ethics.

What we want to do is addressed at the Normative Level of the figure, including risk-based decision making, management and planning, the strategy for making scientific progress and knowledge sharing, legal, and political concerns. We have also positioned the power dimension of the Cyber Game sub-concepts of cooperation (integrative social power), co-option (economic exchange power), and coercion (destructive hard power) at this level.

What we are capable of doing (composed mainly of technology disciplines) is addressed at the Capacity Level of the figure, including the information dimension of the Cyber Game sub-concepts of connection (physical data handling domain), computation (virtual interactivity domain), and cognition (knowledge and meaning domain).

What exists now (the world as it is) is addressed at the Empirical Level of the figure, including physical sciences, computer science, information science, brain sciences, and behavioural and social sciences.

The weak transdisciplinary model is a representation of the safety context of cyberspace. Relevant disciplines are identified at every level and these disciplines must be coordinated to achieve the safety goal in the face of the real-world complexities and conflicts.

Safety through Online Interactivity

This section provides an example of relevant disciplines that are coordinated to achieve safety by linking prospect theory to risk-based decision making in the con-

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

text of cyber-resilience. An important consequence of the example is the notion of safety through online interactivity.

The concept of cyber-resilience (Rütten, 2010) is addressed by Collier and colleagues (2014), who focus on the ability to prepare for and recover quickly from both known and unknown threats. They recommend linking technical data with decision analysis in an adaptable framework to move toward systems that are more resilient to dynamic threats by incorporating decision analysis methods and techniques "to accommodate value-centric perspectives inherent in multiple stakeholder views when addressing the challenge of establishing risk-based standards that will protect the cyber domain" (Collier et al., 2014). This approach is an example of weak transdisciplinarity.

Now consider prospect theory, which is the foundation of the field of behavioural economics. As an evolution of concepts that originate from statistics, economics, and psychology, it is another example that transcends a particular discipline. Using the concept of a reference point to indicate that the human response to losses is stronger than the response to corresponding gains (loss aversion) together with the concept of diminishing sensitivity, it is a coherent theory that can describe decision under risk: prospect theory provides a plausible way to describe different attitudes to risk for gains (as favourable prospects) and losses (as unfavourable propects) (Kahneman, 2011).

Prospect theory should be investigated as at least a partial theoretical grounding of risk-based decision making within the domain of cyber-resilience. It would contribute to descriptions of the behavioural aspects when humans are confronted with decisions "to prepare for and recover quickly from both known and unknown threats". Based on prospect theory, risk-based standards could be enhanced to better align with the decisions humans actually make under such circumstances.

Further, because prospect theory accommodates favourable as well as unfavourable prospects, we believe it applies beyond "risk-based standards that will protect the cyber domain'' (Kahneman, 2011). By accommodating both kinds of prospects, prospect theory in effect could also be considered a theory of decision making pertaining to the duality of risk, which treats each risk situation not just as a threat (an unfavourable propect) but also as an opportunity (a favourable prospect).

As an example from the medical domain (Kahneman, 2011), consider anesthesiologists, who benefit from feedback because their actions are quickly evident, and radiologists, who obtain less immediate information about the accuracy of their diagnoses. In both cases, risk can be considered as the difference between life and death. Saving a patient is an example of a favourable prospect and not saving a patient is an example of an unfavourable prospect. Anesthesiologists and radiologists become better at their profession as they save or do not save patients by continually making decisions under risk and learning and adapting (by modifying their protocol of intervention). Under very different circumstances, both kinds of medical experts must overcome their subjective confidence and must continually know the limits of their expertise as they become more experienced and knowledgeable.

In the context of cyber-resilience, viewing risk as an opportunity is a way to facilitate productive and creative outcomes within a society that is ever more connected on a global scale. When risk as an opportunity is applied within an adaptive learning framework such as the one promoted by Collier and colleagues (2014), online safety becomes a function of user online interactivity. Humans (providing insight and understanding) and systems/networks (interpreting information at scale) will interwork to assess and to achieve joint goals to predict continuously emerging complex phenomena (Bailetti et al., 2014). If such an environment existed, it would make a profound contribution in promoting the future "Progress of Science and useful Arts" (Menard, 2014): cyber-resilience in this sense is not just recovering from individual loss events, but more akin to reduction of brittleness in the protective measures (through an adaptive learning approach).

Conclusion

We presented an approach for addressing safety concerns in the online world of the future using a weak transdisciplinary model, including an initial position about what existing disciplines are most relevant. Although the model does not directly answer key research questions pertaining to underlying safety properties, it does provide a unified structure that accommodates the participation of stakeholders at multiple levels of society and a holistic view.

Instead of restricting the concept of safety (including security) to the protection and control of property, we emphasize improving the safety of cyber-based systems and focus on the intended use of these

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

systems that could lead to profoundly new levels of productivity and creativity for the benefit of society as a whole.

In order to make progress in understanding the underlying properties of safety, and to evolve from the present situation toward the preferable future (Bailetti et al., 2014), attention should be given to applying a methodology of transdisciplinarity that exclusively concentrates on joint problem solving of key research questions pertaining to the science–technology–society triad implied by the weakly transdisciplinary model that was presented. The investigation of prospect theory as a theoretical grounding of risk-based decision making within the domain of cyber-resilience is an example.

We foresee the possibility of a new online environment that becomes progressively safer for participants the more that online interactions occur within the environment. The idea is that a participant's fingerprint is enriched the more that the participant interacts online. The more enriched a participant's fingerprint becomes, the greater the potential for ensuring the safety of the participant. At the same time, the more a participant interacts online, the more opportunity there will be for the participant to be productive and creative.

With this perspective in mind, we believe that future work should contemplate both the productivity and creativity domains in depth to better understand how their respective underlying properties relate to safety when safety is a function of interactivity.

About the Authors

Nadeem Douba is the founding principal of Red Canari, an information security consulting firm that specializes in the areas of information technology and cybersecurity. With over 15 years experience, Nadeem provides consulting and training services for organizations within the public and private sector. He has also presented at some of the world's largest security conferences and is the author of many well-known open source security tools, including one used by the Internet Archive project. His primary research interests include open source intelligence, application and operating system security, and big data. He received his BEng in Systems and Computer Engineering from Carleton University in Ottawa, Canada.

Björn Rütten is the Senior Research Associate for National Security and Public Safety with The Conference Board of Canada. Bjorn leads the Conference Board's research projects in the area of national security and public safety and is responsible for the development and execution of the research plan of the Centre for National Security. He also contributes to other security-related network and research initiatives, such as those of the Centre for the North.

David Scheidl is a recent graduate from the Global Politics program at Carleton University in Ottawa, Canada. During his studies, he focused on security intelligence and geopolitics, with special emphasis on Western security agencies in both the cybersecurity and real-world intelligence fields. He has extensive background in military communications, having served in the Army Signals Reserve since 2009.

Paul Soble is a Science Advisor at the Communications Security Establishment (CSE) in Ottawa, Canada. Over the past three decades, he has held a variety of positions at CSE in the areas of enterprise architecture, visualization and data mining, speech and text natural language processing, adaptive antenna arrays, and systems development. He received his BSc and MSc degrees in Electrical Engineering from University of Manitoba in Winnipeg, Canada, and he is a licensed professional engineer in the province of Ontario.

D'Arcy Walsh is a Science Advisor at the Communications Security Establishment (CSE) in Ottawa, Canada. His research interests include software-engineering methods and techniques that support the development and deployment of dynamic systems, including dynamic languages, dynamic configuration, context-aware systems, and autonomic and autonomous systems. He received his BAH from Queen's University in Kingston, Canada, and he received his BCS, his MCS, and his PhD in Computer Science from Carleton University in Ottawa, Canada.

Safety in the Online World of the Future

Nadeem Douba, Björn Rütten, David Scheidl, Paul Soble, and D'Arcy Walsh

References

Bailetti, T., Levesque, R., & Walsh, D. 2014. The Online World of the Future: Safe, Productive, and Creative. *Technology Innovation Management Review,* 4(10): 5–12. http://timreview.ca/article/834.

Burns, A., McDermid, J., & Dobson, J. 1992. On the Meaning of Safety and Security. *The Computer Journal*, 35(1): 3-15. http://dx.doi.org/10.1093/comjnl/35.1.3

Collier, Z. A., DiMase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. 2014. Cybersecurity Standards: Managing Risk and Creating Resilience. *IEEE Computer,* 47(9): 70-76. http://dx.doi.org/10.1109/MC.2013.448

Jensenius, A. 2012. Disciplinarities: Intra, Cross, Multi, Inter, Trans. ARJ.no. Accessed November 15, 2014. http://www.arj.no/2012/03/

Kahneman, D. 2011. *Thinking, Fast and Slow*. Toronto: DoubleDay Canada.

Kushner, D. 2013. The Real Story of Stuxnet. *IEEE Spectrum,* February 26. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Leveson, N. 2013. *Engineering a Safer World*. Cambridge, MA: MIT Press.

Menand, L. 2014. Crooner in Rights Spat: Are Copyright Laws Too Strict? *The New Yorker,* October 20, 2014. http://www.newyorker.com/magazine/2014/10/20/crooner-rights-spat

Max-Neef, M. A. 2005. Foundations of Transdisciplinarity. *Ecological Economics*, 53(1): 5-16. http://dx.doi.org/10.1016/j.ecolecon.2005.01.014

Nicolescu, B. 2005. Transdisciplinarity – Past, Present, and Future. Il Congresso Mundial de Transdisciplinaridade, 6-12 September, 2005, Brazil. http://cetrans.com.br/textos/transdisciplinarity-past-present-and-future.pdf

Rütten, B. 2010. *Digital Ecosystem Resilience*. Ottawa: The Conference Board of Canada.

Tibbs, H. 2013. *The Global Cyber Game: The Defence Academy Cyber Inquiry Report*. Swindon, UK: Defence Academy of the United Kingdom.

Young, W., & Leveson, N. 2013. System Thinking for Safety and Security. *Proceedings of the 2013 Annual Computer Security Applications Conference (ACSAC 2013).*

Citation: Douba, N., Rütten, B., Scheidl, D., Soble, P., & Walsh, D. 2014. Safety in the Online World of the Future. *Technology Innovation Management Review*, 4(11): 41–48. http://timreview.ca/article/849

Keywords: safety, security, cybersecurity, weak transdisciplinary, prospect theory, risk-based decision making

Author Guidelines

These guidelines should assist in the process of translating your expertise into a focused article that adds to the knowledge resources available through the *Technology Innovation Management Review*. Prior to writing an article, we recommend that you contact the Editor to discuss your article topic, the author guidelines, upcoming editorial themes, and the submission process: timreview.ca/contact

Topic

Start by asking yourself:

- Does my research or experience provide any new insights or perspectives?
- Do I often find myself having to explain this topic when I meet people as they are unaware of its relevance?
- Do I believe that I could have saved myself time, money, and frustration if someone had explained to me the issues surrounding this topic?
- Am I constantly correcting misconceptions regarding this topic?
- Am I considered to be an expert in this field? For example, do I present my research or experience at conferences?

If your answer is "yes" to any of these questions, your topic is likely of interest to readers of the TIM Review.

When writing your article, keep the following points in mind:

- Emphasize the practical application of your insights or research.
- Thoroughly examine the topic; don't leave the reader wishing for more.
- Know your central theme and stick to it.
- Demonstrate your depth of understanding for the topic, and that you have considered its benefits, possible outcomes, and applicability.
- Write in a formal, analytical style. Third-person voice is recommended; first-person voice may also be acceptable depending on the perspective of your article.

Format

1. Use an article template: .doc .odt
2. Indicate if your submission has been previously published elsewhere. This is to ensure that we don't infringe upon another publisher's copyright policy.
3. Do not send articles shorter than 1500 words or longer than 3000 words.
4. Begin with a thought-provoking quotation that matches the spirit of the article. Research the source of your quotation in order to provide proper attribution.
5. Include a 2-3 paragraph abstract that provides the key messages you will be presenting in the article.
6. Provide a 2-3 paragraph conclusion that summarizes the article's main points and leaves the reader with the most important messages.
7. Include a 75-150 word biography.
8. List the references at the end of the article.
9. If there are any texts that would be of particular interest to readers, include their full title and URL in a "Recommended Reading" section.
10. Include 5 keywords for the article's metadata to assist search engines in finding your article.
11. Include any figures at the appropriate locations in the article, but also send separate graphic files at maximum resolution available for each figure.

Issue Sponsor