Technology Innovation Management Review

January 2015

Image licensed under CC BY by woodleywonderworks

Cybersecurity

Welcome to the January 2015 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

About TIM

The TIM Review is the journal of the Technology Innovation Management program (TIM; timprogram.ca), an international graduate program at Carleton University in Ottawa, Canada.

Editorial: Cybersecurity

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

From the Editor-in-Chief

Welcome to the January 2015 issue of the *Technology Innovation Management Review*. The editorial theme of this issue is **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 addition to reading the current issue, we encourage you to revisit our previous four issues on the theme of Cybersecurity:

• July 2013 (timreview.ca/issue/2013/july)

• August 2013 (timreview.ca/issue/2013/august)

• October 2014 (timreview.ca/issue/2014/october)

• November 2014 (timreview.ca/issue/2014/november)

In February, our guest editors will be **Stephen L. Vargo**, **Marja Toivonen**, and **Risto Rajala** for a special issue arising from the 2014 Annual Conference of the European Association for Research on Services (RESER; reser.net), which was held last September in Helsinki, Finland.

Please note that 2015 RESER conference (reser2015.dk) will be held in Copenhagen, Denmark, from September 10–12. The conference theme will be "Innovative Services in the 21st Century", and it will be preceded by a doctoral colloquium (sem.aalto.fi/en/events/reser_dc_2015/) from September 8–9, 2015.

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 has been my pleasure to be the guest editor for five issues of the TIM Review that have examined the theme of Cybersecurity: July and August 2013; October and November 2014; and January 2015. These five issues are the outcomes of a capacity-building initiative led by the VENUS Cybersecurity Corporation (venuscyber.com) and Carleton University (carleton.ca) in Ottawa, Canada. This initiative offers many opportunities for scholarly inquiry and innovative industrial initiatives.

A total of 57 authors contributed 28 articles, 3 Q&As, and 2 summaries of lectures to these five issues. Of these 57 authors, 19 (33%) were from industry, 25 (44%) were from academia, 12 (21%) were from government, and 1 (2%) was from a not-for-profit organization. Fifteen of the 57 authors (26%) were faculty, students, or alumni of Carleton University's Technology Innovation Management (TIM; timprogram.ca) program.

The January 2015 issue of the TIM Review includes four articles and one Q&A. They contribute insights, a method, a model, a case study, and an answer to a question.

Mackenzie Adams is Vice President and Creative Director at SOMANDA, a consulting company. She and **Maged Makramella** are graduate students in the Technology Innovation Management program at Carleton University. In their article, they discuss the use of gamification methods that enable all employees and organizational leaders to play the roles of various types of attackers in an effort to reduce the number of successful attacks due to human vulnerability exploits.

Reza Shirazi is an Analyst Programmer at the Canada Revenue Agency, Information Technology Branch. His article contributes a model to predict the performance of botnet takedown initiatives and a set of hypotheses anchored around the model.

Mohamed Amin is a Solution Architect for Alcatel-Lucent Canada and **Zaid Tariq** is a Senior Network Engineer for Cisco Systems. In their article, they argue that

Editorial: Cybersecurity

Chris McPhee and Tony Bailetti

high intrusiveness by car manufacturers in defining module interfaces and subcomponents for suppliers would lead to more secure cars.

Anas Al Natsheh is at the Centre for Measurement and Information Systems (CEMIS-Oulu) in Oulu, Finland, and at Kajaani University of Applied Sciences, also in Finland. **Saheed Adebayo Gbadegeshin**, **Antti Rimpiläinen**, **Irna Imamovic-Tokalic**, and **Andrea Zambrano** are Project Researchers at the Kajaani University of Applied Sciences in Finland. Their article examines the challenges in commercializing high technologies successfully and sustainably using quantum key distribution (QKD) technology as a case study.

Walter Miron is a Director of Technology Strategy at TELUS Communications. His Q&A answers the question: Should the Internet be considered critical infrastructure?

We encourage the readers of the TIM Review, their colleagues, and their organizations to act decisively to improve the security of cyberspace.

We thank you for reading the journal.

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*, 5(1) 3–4. http://timreview.ca/article/860

Keywords: cybersecurity, employee training, cyber-attacks, gamification, botnets, botnet takedowns, automotive manufacturing, outsourcing, commercialization, quantum key distribution, Internet, critical infrastructure

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

> *"It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle."*
>
> Sun Tzu (544 BC – 496 BC)
> Military general, strategist, and philosopher
> in *The Art of War*

Although cybersecurity awareness training for employees is important, it does not provide the necessary skills training required to better protect businesses against cyber-attacks. Businesses need to invest in building cybersecurity skills across all levels of the workforce and leadership. This investment can reduce the financial burden on businesses from cyber-attacks and help maintain consumer confidence in their brands. In this article, we discuss the use of gamification methods that enable all employees and organizational leaders to play the roles of various types of attackers in an effort to reduce the number of successful attacks due to human vulnerability exploits.

We combine two separate streams – gamification and entrepreneurial perspectives – for the purpose of building cybersecurity skills while emphasizing a third stream – attacker types (i.e., their resources, knowledge/skills, and motivation) – to create training scenarios. We also define the roles of attackers using various theoretical entrepreneurial perspectives. This article will be of interest to leaders who need to build cybersecurity skills into their workforce cost-effectively; researchers who wish to advance the principles and practices of gamification solutions; and suppliers of solutions to companies that wish to build cybersecurity skills in the workforce and leadership.

Introduction

Cybersecurity training is a crucial response to a growing number of intrusions and attacks (Nagarajan et al., 2012). Human vulnerabilities account for 80% of total vulnerabilities exploited by attackers (IBM, 2013) yet the focus of cybersecurity in information technology has been on systems tools and technology (Hershberger, 2014). Human vulnerabilities include, but are not limited to, employee negligence, leadership misinformation and limited cybersecurity skills training, malicious insiders, and third parties who have access to an organization's network. The need to build cybersecurity skills and increase knowledge in the workforce and leadership has become apparent to top corporate decision makers, governmental bodies, and academic researchers (Evans & Reeder, 2010). After the 2013 data breach of Target Corporation, an analysis of the attack concluded that the Target security systems detected the breach but the leadership and employees responsible for taking the steps to respond lacked the necessary skills and knowledge (Hershberger, 2014).

Limited knowledge and skills training in cybersecurity is not unique to Target and it is not an unusual occurrence. A recent study found that almost 70% of critical infrastructure providers across 13 countries suffered a data breach in 2013, and it was found that 54% of those breaches resulted from employee negligence; however, the most unexpected finding was that only 6% of these

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

companies provided cybersecurity training for all employees (Unisys, 2014). Any employee in an organization can be a potential point of entry for attackers; therefore, knowledge and skills training in cybersecurity for all employees is essential in reducing human vulnerabilities. Companies that did not provide security training for new hires reported average annual losses in the amount of $683,000, whereas those who conducted new-hire training reported average annual losses at $162,000 (PwC, 2014).

In general, current cybersecurity skills training are limited to IT personnel while awareness campaigns and education are often offered to all employees. Cybersecurity training for all employees is inefficient in conveying the necessary knowledge and skills for employees and organization leaders to reduce the number of successful attacks. These training approaches can include: web-based classrooms, teleconferencing, instructor-led training, thematic cybersecurity events, newsletters, and awards/incentives programs (Annetta, 2010; Cone, 2007; Nagarajan et al., 2012). These approaches were found to be ineffective because the participants were not engaged in the learning process. The training sessions provided a large amount of information in a short period of time, which created a passive, overwhelming, and disconnected learning experience (Annetta, 2010; Cone, 2007). Classroom instruction and the dissemination of online advice are ineffectual ways to learn; a more immersive and interactive training is required.

In this article, we describe a gamification approach to building cybersecurity skills in all employees and leadership in an organization. Using gamified solutions in cybersecurity skills training promotes active learning and motivation while increasing retention of the learnt skills in comparison to traditional learning approaches such as instructor-led classes (Jordan et al., 2011).

The gamification approach uses entrepreneurial perspectives, which complement attacker types based on their motivation, knowledge, and resources. We use entrepreneurial perspectives, which refer to characteristics of seeking opportunities, taking risks, and having the focus to pursue an idea to fruition (Kuratko, 2013), to help view the challenge through the eyes of cyber-attackers. Some of the similarities drawn between hackers and entrepreneurs include their problem-solving capabilities, willingness to take advantage of opportunities, working hard, as well as taking risks (Blanchard, 2013; Kang, 2012; Warikoo, 2014).

In the remainder of the article, we examine the use of gamification to develop employee skills and identify various entrepreneurial perspectives that are relevant to this approach. Then, we discuss what is required to create a training approach that uses gamification to deliver immersive learning in cybersecurity. In the final section, we provide conclusions.

Using Gamification to Build Skills in Employees

Gamification is a process of enhancing a specific service by implementing game design elements in a non-game context to enhance the user's overall value creation and experience (Huotari & Hamari, 2011; Deterding et al., 2011). Deterding and colleagues (2011) define gamification as "the use of design elements characteristic for games in non-game contexts". Thus, gamification reflects the use of game thinking including progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem solving, stories, and competition in non-game situations (Deterding et al., 2011; Kapp, 2012). Underlying gamification is an understanding of motivation as significantly correlated with and predictive of desirable human outcomes such as achievement, success, and the attainment of distinction and rewards (Kapp, 2012). When designed and applied in an appropriate manner and setting, gamification provides an alignment between motivation and desire that leads to the anticipated purpose of its use. For instance, when used to increase employee engagement, gamification can improve teamwork and transform routine, often dull, tasks by motivating employees through "play" and competition within the same team and across teams (Korolov, 2012; Zichermann & Cunningham, 2011).

Although it is usually considered an effective user involvement tool, gamification can also be used to develop skills of participants and employees. Burke (2014) highlights the effectiveness of using gamification concepts in employee training while using the "Ignite Leadership Game" created by NTT Data as a relevant example. This specific gameful design is built on first assessing the employees' knowledge to identify their strengths and weaknesses; the identification allows them to develop the required skill sets more efficiently. The main benefits of using gamification approaches to develop skills are creating an atmosphere that enables employee active involvement (Zichermann & Linder, 2013), improving the participants' motivation to achieve better results (Burke, 2014), and enhancing the overall learning process due to the established collaborative environment (Burke, 2014).

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

Gamification elements

When designing games for training and educational purposes, training goals must be clearly defined (Nagarajan et al., 2012). Designing effective and relevant games requires the selection of the appropriate gamification elements that would best suit the training approach needed (Kapp, 2012). Four elements of gamification are highlighted below for cybersecurity skills training:

1. *Progress mechanics:* related to player motivation through the provision of progress tools such as points, leader boards, and badges.

2. *Player control:* the use of a character (a third-person perspective) to engage in the gamified training. This character is commonly known as an "avatar". Research has shown that the use of avatars, through the use of different roles, influences behaviour.

3. *Problem solving:* a crucial element in gamification when learning and retaining new information is the goal of the training. Collaboration and identification of a shared purpose are essential in developing strong problem-solving skills that can easily translate into practical knowledge outside of the training environment.

4. *Story:* A narrative that is present to create an attachment or a bond between the learner and their avatar, as well as a bond between the avatars participating in the gamified training. Stories also motivate the learner to keep on "playing" to find out the rest of the story

Existing gamification training solutions

Currently, a handful of cybersecurity training and awareness programs started to introduce gamification techniques in their own curricula. As shown in Table 1, six main, and most evolved, gamified approaches were identified and further elaborated. These "games" were compared according to the following four aspects:

Table 1. Existing gamified training solutions for employee cybersecurity skills

	Awareness	Defensive Strategies	Offensive Strategies	Attacker Centricity	References
CounterMeasure	• Basic knowledge	• *None*	• Authentication and password bypassing	Limited	Jordan et al. (2011)
CyberCiege	• Basic knowledge • General assessment	• Penetration prevention	• *None*	*None*	Cone et al. (2007)
CyberNexs	• *None*	• System assessment • Penetration prevention	• Capture the flag	*None*	Nagarajan et al. (2012)
CyberProtect	• Basic knowledge • General assessment	• *None*	• *None*	*None*	Labuschagne et al. (2011)
NetWars	• Skill assessment	• System assessment • Penetration prevention	• System penetration scenarios	Limited	SANS (2015)
Micro Games	• Basic knowledge • General assessment	• Penetration detection • Password management	• *None*	*None*	Wombat (2015)

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

1. *Awareness:* requires a minimal amount of knowledge for the participants. Awareness is mainly concerned with assessing the level of vulnerabilities in an entity, while providing participants with general knowledge in detecting and avoiding successful penetration attempts.

2. *Defensive strategy:* requires the participants – in this case the defenders – to have substantial knowledge that will provide them with proper tools and strategies to fend off cyber-attacks efficiently.

3. *Offensive strategy:* focuses mainly on putting the participants in their rivals' shoes in order to properly understand their strategies and approaches.

4. *Attacker centricity:* uses known characteristics of cyber-attackers to train participants in anticipating an attacker's motivation and behaviour in carrying out certain attacks. This anticipation enhances the creation and application of both offensive and defensive strategies against cyber-attacks.

Note that only three of the six gamified training programs incorporate offensive strategies for their participants. This observation is in line with the current dominant practice in cybersecurity to react, largely, to attacks and not engage in anticipatory or offensive strategies. Moreover, two of the six games have limited attacker-centricity, mostly based on the skills of hacking a system but not specific attacker types. Once again, this reflects a current state in cybersecurity training where the characteristics of attackers are seldom incorporated in training employees to understand these attackers or anticipate their attacks.

Attacker Types and Their Characteristics

Based on an extensive search of existing literature, and to the best of our knowledge, there are no current applications of cyber-attacker characteristics being used in gamified cybersecurity skills training for employees. As a result, we reviewed literature on cyber-attackers based on a search that included the following keywords: "cyber criminals", "insiders", and "hackers". We expanded our keyword search to accommodate the terminology differences in existing literature when describing individuals or groups that commit cyber-attacks. We focused on cyber-attackers to identify attacker types and their motivations, resources, and knowledge/skills. Identifying attacker types is important in developing more accurate profiles when creating and implementing solutions intended to reduce cybercrimes (Rogers, 2011).

Based on the literature review, the following eight types of cyber-attackers were identified:

1. *Script kiddies:* attackers who depend on existing tools (e.g., exploit programs and scripts) and are unwilling to learn how these tools function (Hald & Pedersen, 2012). They are immature attackers whose primary motivation is to create mischief and get attention (Aggarwal et al., 2014; Rogers, 2011).

2. *Cyber-punks* (including virus writers): attackers who write viruses and exploit programs for the sake of causing trouble and gaining fame (Hald & Pedersen, 2012). Motivated by admiration and recognition, these attackers disrespect authority and social norms. They are only slightly more skilled than script kiddies (Rogers, 2011) and enter systems to cause damage (Dogaru, 2012).

3. *Insiders:* attackers who are imbedded within the organization they attack who cause intentional or unintentional harm because of their authorized access (Hald & Pedersen, 2012). Because access is not a challenge they face, most insider attackers have minimal technical skills (Williams, 2008). As such, they become easy targets for criminals who persuade them to perform an action that exposes the system (Crossler et al., 2013; Parmar, 2013).

4. *Petty thieves:* attackers who commit online fraud such as identity theft and system hijackings for ransom with no other motivation than money (Hald & Pedersen, 2012). Their activities are not sophisticated and they are not dependent on the gains from their crimes. They are attracted to criminal activities that include credit card and bank fraud (Rogers, 2011).

5. *Grey hats:* attackers who are a mix of black hats (i.e., malicious or illegal hackers) and white hats (i.e., hackers intending to improve security). They may attack systems to prove their abilities or to find flaws within a system, and may alert the target to the vulnerability (Aggarwal et al., 2014; Bodhani, 2013; Hald & Pedersen, 2012). Often highly skilled, they write scripts that cyber-punks and script kiddies typically employ (Rogers, 2011).

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

6. *Professional criminals:* attackers who are hired to infiltrate systems. They are also known as cyber-mercenaries (Hald & Pedersen, 2012). Sometimes these cyber-attackers act on behalf of institutions and enter competitors' systems for financial gain (Dogaru, 2012). They operate in the most secretive environment and are governed by strict rules of anonymity so they cannot be identified (Kowalski & Mwakalinga, 2011; Rogers, 2011).

7. *Hactivists:* attackers who are motivated by ideology. This type can include terrorist groups. Pushed into activism by strong psychological dispositions and beliefs, some hackers may become hacktivists and perceive their motives to be completely selfless (Hald & Pedersen, 2012; Papadimitriou, 2009).

8. *Nation states:* attackers who are assumed to be working on behalf of a governmental body. Every resource is targeted towards the disruption of the enemy's systems or the protection of the nation state's own systems. This group includes paramilitary organizations and freedom fighters, and their goals are not dissimilar to those of recognized governments (Dogaru, 2012; Hald & Pedersen, 2012; Rogers, 2011).

It is important to note a common theme found in hacker communities: willingness to share information and collaborate in problem solving with peers (Biros et al., 2008; Denning, 1996; Jordan & Taylor, 1998; Mookerjee et al., 2009). Sharing information helps build stronger bonds within the community while encouraging and challenging others to learn and engage more (Arief & Besnard, 2003).

Entrepreneurial Perspectives

Entrepreneurs are described as risk takers, innovators, and problem solvers who are confident, persistent, collaborative, able to recognize opportunities, skilled at gathering information and knowledge, have a need for achievement and reward, and seek change and profit (Blanchard, 2013; Kang, 2012; Kim, 2014). Although there are many definitions of the term "entrepreneur", the following definition is most apt for this article: entrepreneurs are "those who identify a need – *any* need – and fill it. It's a primordial urge, independent of product, service, industry, or market" (Nelson, 2012). Thus, it can be inferred that this primordial urge is driven by different motivations and capabilities, which may be better understood through entrepreneurial perspectives.

Entrepreneurial perspectives are examined in this article for two reasons: i) to consider the similarities between various entrepreneurial perspectives and cyber-attacker characteristics and ii) to remove the negative connotation connected to the term "attacker" in the training. Taking the perspective of someone about whom an individual has negative perceptions and attitudes may compromise the in-depth immersion into a cyber-attacker's motivation and approach, and reduce "buy-in" to the gamification approach to training. Thus, taking an entrepreneurial perspective helps trainees empathize with cyber-attackers so that they may better learn to protect their organizations against them.

From the literature, we identified the following six entrepreneurial perspectives:

1. *Bricolage:* a perspective where an entrepreneur uses whatever diverse resources happen to be at hand to start a new venture. The concept was originally used in artistic contexts and usually starts in an environment with limited resources (Baker & Nelson, 2005). This perspective requires creativity, and the resulting innovations may need several testing stages before then come to fruition.

2. *Effectuation:* a perspective where an entrepreneur takes "a set of means as given and focus[es] on selecting between possible effects that can be created with that set of means" (Saravathy, 2001). This perspective connotes that an entrepreneur is considered as highly knowledgeable in using their own resources. That is, they may not have access to a large amount of resources, but they are considered experts in utilizing their available resources in many innovative ways.

3. *Causation:* a perspective whereby an entrepreneur focuses on a specific goal that is highly desired and uses all the available resources to reach this certain goal. In this perspective, the setting itself is usually rich in resources which requires high knowledge in how to use these resources to achieve optimal results and achieve greater outcomes (Sarasvathy, 2001).

4. *Emancipation:* a perspective where a person, who is suffering from some kind of physical or emotional oppression, decides to break free to improve their situation. It can also apply to improving the situation in their area, community, or even country. Rindova and colleagues (2009) identified three core elements of emancipation: seeking autonomy, authoring, and making declarations.

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

5. *Hubris:* a perspective in which an entrepreneur's belief in the success of a new venture is based on socially constructed confidence (Hayward et al., 2006). An optimistic overconfidence propels the individual to start a venture regardless of the potential failure.

6. *Social:* a perspective where an entrepreneur's main motivations are social goals (social, political, environmental) and sharing part of their gained resources with community causes (Christopoulos & Vogl, 2015).

Proposed Gamification Approach to Build Cybersecurity Skills

Cybersecurity training is mislabelled in most organizations; it should be more appropriately referred to as cybersecurity information and awareness training that is provided to all employees. Cybersecurity skills training is mostly offered to highly technical IT administration and security professionals. All employees need foundational skills training with customizations to tailor scenarios based on functional roles and potential attack vectors with an emphasis on learning how to mitigate or cope with an attack (Council on Cybersecurity, 2014).

Based on our review of the literature, we propose a gamified approach to cybersecurity skills training. Using the elements of gamification, we outline four components required to create a comprehensive cybersecurity skills training: i) story, ii) player control, iii) problem solving, and iv) progress mechanics.

Story
The stories of the training games will be based on the eight identified cyber-attacker types and they will provide realistic, virtual recreations of the work environment and simulate the types of attacks that may occur. For this gamified cybersecurity training, there are three relevant components that help keep the trainees engaged and motivated:

1. *Feedback:* such as losing lives, triggering warning screens, receiving encouraging messages, or earning rewards. This feedback is based on the trainee's progress: as long as they are engaged in the game, the game is providing feedback, assessing skill levels, and creating obstacles to evaluate the various skillsets of the trainees and comparing those results to the target level of achievement.

2. *Increased challenges:* the complexity of the story will dictate the amount of challenges the trainee will have to overcome in order to progress.

3. *Opportunities for mastery:* providing opportunities to develop and excel.

Player control
The six entrepreneurial perspectives are used to create resource- and motivation-based attacker roles for the training solution. The entrepreneurial perspectives are matched to the attacker types as shown in Table 2. This step enables avatars to be created for the game without any preconceived notions on how the avatar should act, thereby allowing for exploratory learning in the scenarios.

Problem solving
Problem solving is an important element in gamification that allows trainees to learn and retain new information. As trainees collaborate to find answers, they create a community of shared information and purpose. Such activities are particularly helpful during attacker-centric cybersecurity skills training due to the collaborative nature of the cyber-attacker community and its ability to find common goals.

Progress mechanics
For all employees and organization leaders participating in the gamified training, the progress mechanics will vary based on the avatar's characteristics and areas of learning and achievements. For example, if an employee's avatar is "the architect" as listed in Table 2, a quick review of their in-game resources would show that the avatar has many resources available for them to complete a task so the challenge in gaining more resources or points may be linked more to problem solving skills or collaboration efforts.

Gamified Training Scenario

To understand how the training would be used and what the expected learning outcomes are, consider the following scenario. A graphic designer in the marketing department must complete his cybersecurity skills training. At the beginning of the training, he is given a short knowledge-assessment questionnaire. Based on his answers, he is assessed as having "average" cybersecurity knowledge, which would then determine his entry level in the training game. He is then given the option to choose an avatar with very little descriptive information about the avatar such as its strengths, weaknesses, and resources to progress along in the game. He selects "The advocate" as his avatar and, based on his assessment, he begins at level 2 of the training. The story he will work through is based on "The hacktivist" attacker type and an attack type of en-

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

Table 2. Gamification element: player control (avatars and their characteristics)

Avatars (Attacker Roles)	Avatar Characteristics (Attacker Types)
Bricolage: "The rookie"	• Script kiddies • Cyber-punks • Petty thieves
Effectuation: "The adroit"	• Insiders
Causation: "The architect"	• Nation states • Professional criminals
Emancipation: "The liberator"	• Insiders • Hacktivists
Hubris: "The optimist"	• Grey hats
Social: "The advocate"	• Hactivists

tering a secure area by following an employee who entered using their own access key to plant malware in one of the computers in a certain department. As he progresses through the game, he may need to collaborate with other trainees or other avatars in the game to complete a mission or a step. As he progresses along, there is information provided such as warnings, hints, and other learning opportunities to successfully complete the level. There are different rewards and incentives provided to keep him engaged and motivated.

By the end of this training, the employee is able to plant the malware after a few failed attempts. During the training, the employee learns the desired skills, progressing from prevention to anticipation to reaction to response, as described below:

1. *Prevention:* the importance of securing access against unauthorized individuals when entering secure areas.

2. *Anticipation:* a method used by some attackers to gain access to the system.

3. *Reaction:* the importance of communication with others in the organization.

4. *Response:* the proper procedure to follow when confronted with a similar situation. The impact of a successful attack.

In comparison, instructor-led classroom training would have provided the information to the trainee without any practical, hands-on activities to show the steps involved or to visually witness the impact of the security breach. It would also be difficult for the trainee to retain the procedural information to deal with this type of issue. Most importantly, it is difficult to keep the attention of the employee on the training material without the interactive and immersive game element.

The gamified cybersecurity skills training approach promotes:

1. The prevention > anticipation > reaction > response sequence

2. Skills training for all employees in an organization, from entry-level staff to C-level executives

3. Hands-on, immersive, and interactive training that moves away from classroom-based, instructor-led training

4. A distinction between cybersecurity awareness only training and cybersecurity skills training

Conclusion

The main objective of this article was to provide an innovative approach to train all employees and organization leaders to develop cybersecurity skills and better defend against and react to data breaches. The gamified training approach was developed by reviewing the following literature streams: gamification, cyber-attackers and their characteristics, and entrepreneurial perspectives.

In this article, eight attacker types were selected using their motivation, knowledge/skills, and resources as attacker characteristics. Furthermore, six entrepreneurial perspectives were used highlighting their motivation, knowledge/skills, and resources. The attacker types and their characteristics were combined with the entrepreneurial perspectives to create avatars for the game. By creating the avatars, the type of attacker and the characteristics of the attacker are now used in creating the story used during the training. This approach allows the trainees to experience an attack through the eyes of a cyber-attacker and therefore from entrepreneurial perspectives.

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

Our article is limited by the lack of practical, tested evidence that the approach would produce the expected outcomes and improve employees' abilities in preventing or reacting to data breaches. Some of the research has pointed to the importance of identifying attacker characteristics to better defend against cyber-attacks (Colwill, 2009; Cremonini & Nizovtsev, 2006; Gold, 2011; Liu & Cheng, 2009), and further research linking the attacker characteristics to the attack type may advance knowledge in cybersecurity prevention and training. We would also recommend a more comprehensive project that examines the similarities and differences between entrepreneurs and attackers.

About the Authors

Mackenzie Adams is a serial entrepreneur, a Senior Technical Communicator, and a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She is also a VP/Creative Director at SOMANDA, a consulting company. Over the past 15 years, Mackenzie has worked in a variety of fields ranging from social work to accounting and has used those experiences to develop strong strategic and analytical skills. She is interested in the fields of artificial intelligence and quantum computing, and how they relate to cybersecurity.

Maged Makramalla is a current graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. He holds a Bachelor of Science degree in Mechatronics Engineering from the German University in Cairo, Egypt. For three years, he has been working as Manager of the Sales and Marketing Department of TREND, a trading and engineering company based in Cairo. His primary research interest lies in the improvement of educational techniques by introducing experiential learning into the regular curriculum while promoting gamification of educational methods.

References

Aggarwal, P., Arora, P., & Ghai, R. 2014. Review on Cyber Crime and Security. *International Journal of Research in Engineering and Applied Sciences,* 2(1): 48–51.

Annetta, L. A. 2010. The "I's" Have It: A Framework for Serious Educational Game Design. *Review of General Psychology,* 14(2): 105–112. http://dx.doi.org/10.1037/a0018985

Arief, B., & Besnard, D. 2003. *Technical and Human Issues in Computer-Based Systems Security.* Technical Report Series: University of Newcastle upon Tyne Computing Science. Newcastle, UK: Newcastle University.

Baker, T., & Nelson, R. E. 2005. Creating Something from Nothing: Resource Construction through Entrepreneurial Bricolage. *Administrative Science Quarterly,* 50(3): 329–366. http://dx.doi.org/10.2189/asqu.2005.50.3.329

Biros, D. P., Weiser, M., Burkman, J., & Nichols, J. 2008. Information Sharing: Hackers vs Law Enforcement. In *Proceedings of the 9th Australian Information Warfare and Security Conference.* Perth, Australia: Edith Cowan University.

Blanchard, K. 2013. Entrepreneurial Characteristics in SMEs: A Rural, Remote Rural, and Urban Perspective of Lincolnshire Businesses. *Strategic Change,* 22(3/4): 191–201. http://dx.doi.org/10.1002/jsc.1932

Bodhani, A. 2013. Bad... In a Good Way. Engineering & Technology, 8(12): 64–68. http://dx.doi.org/10.1049/et.2012.1217

Burke, B. 2014. *Gamify: How Gamification Motivates People to Do Extraordinary Things.* Brookline, MA: Bibliomotion, Inc.

Chiang, O. 2010. Wombat Security Makes Online Games That Teach Cybersecurity Awareness, Nabs $750,000 US Airforce Contract. *Forbes Magazine.* Accessed January 10, 2015: http://www.forbes.com/sites/oliverchiang/2010/10/08/wombat-security-makes-videogames-that-teach-cybersecurity-awareness-nabs-750000-us-airforce-contract/

Christopoulos, D., & Vogl, S. 2015. The Motivation of Social Entrepreneurs: The Roles, Agendas and Relations of Altruistic Economic Actors. *Journal of Social Entrepreneurship*, 6(1): 1–30. http://dx.doi.org/10.1080/19420676.2014.954254

Colwill, C. 2009. Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days? *Information security Technical Report,* 14(4): 186–196. http://dx.doi.org/10.1016/j.istr.2010.04.004

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. 2007. A Video Game for Cyber Security Training and Awareness. *Computers & Security,* 26(1): 63–72. http://dx.doi.org/10.1016/j.cose.2006.10.005

Council on CyberSecurity. 2014. *The Critical Security Controls for Effective Cyber Defense.* Version 5.1. Council on CyberSecurity. Accessed January 10, 2015: http://www.counciloncybersecurity.org/

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

Cremonini, M., & Nizovtsev, D. 2006. *Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies.* Presented at The Fifth Workshop on the Economics of Information Security (WEIS), 26–28 June 2006. Cambridge, UK: The University of Cambridge. http://weis2006.econinfosec.org/docs/3.pdf

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. 2013. Future Directions for Behavioral Information Security Research. *Computers & Security,* 32, 90–101. http://dx.doi.org/10.1016/j.cose.2012.09.010

Denning, D. E. 1996. Concerning Hackers Who Break into Computer Systems. In P. Ludlow (Ed.), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace:* 137–164. Cambridge, MA: MIT Press

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. 2011. From Game Design Elements to Gamefulness: Defining Gamification. In *Proceedings of the 15th International Academic MindTrek Conference:* 9–15. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/2181037.2181040

Dogaru, P. D. S. O. 2012. Criminological Characteristics of Computer Crime. *Journal of Criminal Investigation,* 5(1): 92-98.

Gold, S. 2011. Understanding the Hacker Psyche. *Network Security,* 2011(12): 15–17. http://dx.doi.org/10.1016/S1353-4858(11)70130-1

Hald, S. L., & Pedersen, J. M. 2012. An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties. In *Proceedings of the 14th IEEE International Conference on Advanced Communication Technology (ICACT):* 81–86. Pyeongchang, South Korea: IEEE.

Hershberger, P. 2014. *Security Skills Assessment and Training: The "Make or Break" Critical Security Control.* SANS Institute InfoSec Reading Room. Accessed January 10, 2015: http://www.sans.org/reading-room/whitepapers/leadership/security-skills-assessment-training-critical-security-control-break-o-35637

Huotari, K., & Hamari, J. 2012. Defining Gamification: A Service Marketing Perspective. In *Proceedings of the 16th International Academic MindTrek Conference:* 17–22. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/2393132.2393137

Hayward, M. L., Shepherd, D. A., & Griffin, D. 2006. A Hubris Theory of Entrepreneurship. *Management Science,* 52(2): 160–172. http://dx.doi.org/10.1287/mnsc.1050.0483

Jordan, C., Knapp, M., Mitchell, D., Claypool, M., & Fisler, K. 2011. CounterMeasures: A Game for Teaching Computer Security. In *Proceedings of the 10th Annual Workshop on Network and Systems Support for Games:* Article 7. Piscataway, NJ: IEEE Press.

Jordan, T., & Taylor, P. 1998. A Sociology of Hackers. *The Sociological Review,* 46(4): 757–780. http://dx.doi.org/10.1111/1467-954X.00139

Kang, H. 2012. The Entrepreneur as a Hacker. *Epicenter: National Center for Engineering Pathways to Innovation.* Accessed January 10, 2015. http://epicenter.stanford.edu/story/hongwen-henry-kang-carnegie-mellon-university

Kapp, K. M. 2012. *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education.* San Francisco, CA: Pfeiffer (Wiley).

Kim, P. H. 2014. Action and Process, Vision and Values. In T. Baker & F. Welter (Eds.), *The Routledge Companion to Entrepreneurship,* 59–74. New York, NY: Routledge.

Korolov, M. 2012. Gamification of the Enterprise. *Network World.* Accessed January 10, 2015: http://www.networkworld.com/article/2160336/software/gamification-of-the-enterprise.html

Kuratko, D. 2013. *Entrepreneurship: Theory, Process, and Practice.* Melbourne, Australia: Cengage Learning.

Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M. 2011. Design of Cyber Security Awareness Game Utilizing a Social Media Gramework. In *Information Security South Africa,* 1–9. Johannesburg, SA: IEEE. http://dx.doi.org/10.1109/ISSA.2011.6027538

Liu, S., & Cheng, B. 2009. Cyberattacks: Why, What, Who, and How. *IT Professional, 1*1(3): 14–21. http://dx.doi.org/10.1109/MITP.2009.46

Mwakalinga, G. J., & Kowalski, S. 2011. *Modelling the Enemies of an IT Security System-A Socio-Technical System Security Model.* Presented at The 12th International Symposium on Models and Modeling Methodologies in Science and Engineering. March 27–30, 2011: Orlando, FL.

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. 2011. When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. *Information Systems Research,* 22(3): 606–623. http://dx.doi.org/10.1287/isre.1100.0341

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. 2012. Exploring Game Design for Cybersecurity Training. In *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER): 256–262.* May 27–31, 2012, Bangkok, Thailand. http://dx.doi.org/10.1109/CYBER.2012.6392562

Nelson, B. 2012. The Real Definition of Entrepreneur – And Why It Matters. *Forbes.* Accessed January 10, 2015: http://www.forbes.com/sites/brettnelson/2012/06/05/the-real-definition-of-entrepreneur-and-why-it-matters/

Parmar, B. 2013. Employee Negligence: The Most Overlooked Vulnerability. *Computer Fraud & Security,* 2013(3): 18–20. http://dx.doi.org/10.1016/S1361-3723(13)70030-7

PwC. 2014. *US Cybercrime: Rising Risks, Reduced Readiness – Key Findings from the 2014 US State of Cybercrime Survey.* PricewaterhouseCoopers, CERT Division of the Software Engineering Institute, CSO Magazine, & United States Secret Service.

Rindova, V., Barry, D., & Ketchen, D. J. 2009. Entrepreneuring as Emancipation. *Academy of Management Review,* 34(3): 477–491. http://dx.doi.org/10.5465/AMR.2009.40632647

Rogers, M. K. 2011. The Psyche of Cybercriminals: A Psycho-Social Perspective. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis:* 217–235. New York, NY: Springer. http://dx.doi.org/10.1007/978-3-642-13547-7_14

SANS. 2015. NetWars. *SANS Institute.* Accessed January 10, 2015: http://sans.org/netwars

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

Sarasvathy, S. D. 2001. Causation and Effectuation: Toward a Theoretical Shift from Economic Inevitability to Entrepreneurial Contingency. *Academy of Management Review,* 26(2): 243–263. http://dx.doi.org/10.5465/AMR.2001.4378020

Unisys. 2014. Critical Infrastructure: Security Preparedness and Maturity. *Unisys.* Accessed January 10, 2015: http://www.unisys.com/insights/critical-infrastructure-security

Warikoo, A. 2014. Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective,* 23(4-6): 172–178. http://dx.doi.org/10.1080/19393555.2014.931491

Williams, P. A. H. 2008. In a 'Trusting' Environment, Everyone Is Responsible for Information Security. *Information Security Technical Report,* 13(4): 207–215. http://dx.doi.org/10.1016/j.istr.2008.10.009

Wombat. 2015. Security Education Platform. *Wombat Security Technologies.* Accessed January 10, 2015: http://wombatsecurity.com/security-education

Zichermann, G., & Cunningham, C. 2011. *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps.* Sebastopol, CA: O'Reilly Media.

Citation: Adams, M., & Makramalla, M. 2015. Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, 5(1): 5–14. http://timreview.ca/article/861

Keywords: cybersecurity, cyber attackers, gamification, entrepreneur, training

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

> *"Men rise from one ambition to another: first, they seek to secure themselves against attack, and then they attack others."*
>
> Niccolò di Bernardo dei Machiavelli (1469–1527)
> Historian, politician, diplomat, philosopher, and humanist

Botnets have become one of the fastest-growing threats to the computer systems, assets, data, and capabilities relied upon by individuals and organizations worldwide. Botnet takedown initiatives are complex and as varied as the botnets themselves. However, there is no comprehensive database of botnet takedowns available to researchers and practitioners, nor is there a theoretical model to help predict the success or failure of future takedown initiatives. This article reports on the author's ongoing research that is contributing to both of these challenges and introduces a set of hypotheses relating to the performance of botnet takedown initiatives. In addition to researchers, the article will be of particular interest to personnel in technical, legal, and management functions of organizations interested in improving the quality of their communications and accelerating decision making for the purpose of launching and operating botnet takedown initiatives. It will also be of interest to entrepreneurs who wish to launch and grow cybersecurity ventures that provide solutions to botnet and malware threats.

Introduction

Botnets are a persistent threat to all Internet users. They are networks of computers infected with malicious software that are connected over the Internet and can be instructed to carry out specific tasks – typically without the owners of those computers knowing it (Nadji et al., 2013; Plohmann et al., 2011; Whitehouse, 2014). Those who control botnets use them to steal identities, personal and financial information, illicitly gain access to bank accounts; distribute spam e-mails; shut down websites by overwhelming them with traffic (i.e., distributed denial-of-service or DDoS attacks); launch new custom-made botnets; or spread malware and ransomware (Cremonini & Riccardi, 2009; Plohmann et al., 2011; Zeidanloo et al., 2010).

Over the last 20 years, botnets have developed "from a subject of curiosity to highly sophisticated instruments" for illegal activities (Czosseck et al., 2011). Botnets increase the computing resources available to cybercriminals exponentially without revealing their identities (Feily et al., 2009; Whitehouse, 2014). Stealth, resilient, and cost-effective botnets have been designed to operate using general overlay networks such as those offered by Skype (Nappa, et al., 2010).

Botnets are difficult to track, disrupt, and dismantle because they operate in various time zones, languages, and laws (Abu Rajab et al., 2006; Schaffer, 2006). Botnet takedown initiatives refer to the actions that lead to the identification and disruption of the botnet's command-and-control infrastructure. The literature on botnet takedowns includes studies on accelerating the botnet takedown process (Nadji et al., 2013), employing botnet takedown methods (Dagon et. al., 2007; Freiling et al., 2005), minimizing botnet profitability (Tiirmaa-Klaar et al., 2013a), and detecting botnets (Dittrich, 2012; Nappa et al., 2010; Zeidanloo et al., 2010; Zhao et al., 2009). Studies have also looked at the managerial implications of botnet takedowns (Borrett et al., 2013; Scully, 2013), botnet lifecycles (Kok & Kurz, 2011), botnet types (Czosseck et al., 2011; Dagon et al., 2007), and practices to prevent and respond to botnet threats (Plohmann et al., 2011). However, there is no comprehensive database of botnet takedowns available to researchers and practitioners, nor is there a theoretical model to help predict the success or failure of future takedown initiat-

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

ives. This article reports on the author's ongoing research that is contributing to both of these challenges and introduces a set of hypotheses relating to the performance of botnet takedowns.

Developing a Database of Botnet Takedown Initiatives

As of late 2014, a readily accessible comprehensive database on botnet takedown initiatives was not available. Responding to the need to develop such a resource, a Google search (using keywords such as "botnet takedown", "botnet disruption", and "botnet dismantled") was conducted, which returned data from various sources, including: recent hearings on crime and terrorism (e.g., Whitehouse, 2014); lists of botnets that appear in large public websites (e.g., Wikipedia, 2014); websites of major IT firms (e.g., Microsoft), cybersecurity institutes (e.g., Symantec), and news agencies; and academic journals and conference proceedings.

Based on the data from these sources, a preliminary database of 19 botnet takedown initiatives was created. The database is being developed and maintained by the Technology Innovation Management program (TIM; timprogram.ca) at Carleton University in Ottawa, Canada, and it will be made publicly available once it is sufficiently mature. Table 1 summarizes the botnets and malware listed in the database, including each botnet's name (alias), its date of discovery, the date its takedown initiative began, its estimated size, and its purpose or tasks performed. However, the full database captures the following additional dimensions about the botnets and their associated takedown initiatives: unique features, means of dissemination, vulnerabilities exploited, responsible entity, impact, takedown leader, takedown process, involvement of authorities, legal issues, and timeline of key dates. As research progress and understanding of consequential dimensions grows, these dimensions will be refined.

Botnet Takedown Performance Model

Informed by the evolving database on botnet takedown initiatives described in the previous section, this study proposes a botnet takedown model to enable diverse, proficient individuals working in IT organizations to understand botnet takedown initiatives. Because there are no existing models to explain the performance of botnet takedowns, Ferrier's (2001) model of the drivers and consequences of competitive aggressiveness on business was used as a starting point to construct an effective barrier against the economic growth of botnets. Ferrier's process model of competitive interaction aims to describe characteristics of forces that influence competitive aggressiveness and the consequential organizational performance. Building on Ferrier's (2001) study, the new two-part model is summarized in Figure 1.

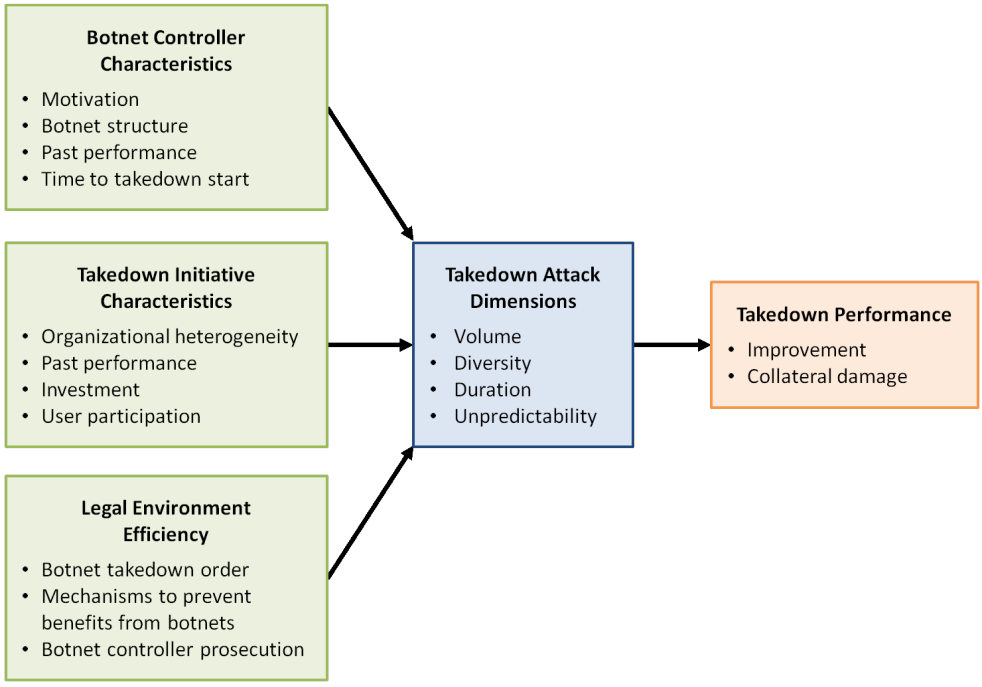

Figure 1. Botnet takedown performance model. Adapted from Ferrier (2001).

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

Table 1. Summary of botnets and malware listed in the preliminary database of takedown initiatives

	Botnet Alias	Date Discovered	Date Takedown Disclosed	Estimated Size	Purpose
1	Bamital botnet	2010 (June)	2013 (Feb 6)	8 million bots	Hijack search results; perpetrate click frauds; direct traffic to selected websites
2	Blackshades malware	2012 (June 19)	2014 (May)	500+ thousand computers in 100 countries	Distribute malware used to control the webcam to turn PC into a surveillance/spy device; record keystrokes to steal usernames and passwords for online accounts (e.g., login into bank accounts; make unauthorized money transfers); encrypt files and demand ransom to unlock them
3	BredoLab botnet (Oficla)	2009 (May)	2010 (Oct)	30 million bots	Lease parts of botnets to enable fraudulent activities of others
4	Citadel malware	2012 (Jan)	2013 (Jun 5)	1,462 botnets	Spread malware to manage bots
5	Coreflood botnet	2001	2011 (Apr 13)	2 million bots	Withdraw money from bank accounts; steal private personal financial information
6	Cryptolocker malware	2013 (Sep)	2014 (May)	500 thousand victims	Encrypt files and then demand payment for decryption
7	Cutwail botnet	2007	2009 (June) 2010 (August)	1.5 to 2.1 million bots	Send unsolicited traffic; rent for others to send unsolicited traffic; deliver DDoS attacks
8	Gameover Zeus botnet	2011 (Sep)	2014 (June)	500 thousand to 1 million bots	Commit bank fraud; distribute other malware using "man-in- the-middle" attacks; distribute CryptoLocker malware
9	Grum botnet (Tedroo, Reddyb)	2009	2012 (July 19)	560-840 thousand bots	Send unsolicited traffic, particularly about pharmaceutical products
10	Kelihos botnet (Waledac 2.0 or Hlux)	2010	2011, 2012 (Several)	300 thousand bots	Steal Bitcoin wallets; send unsolicited emails; deliver DDoS attacks
11	Lethic botnet	2008	2010 (January)	260 thousand bots	Send unsolicited traffic, particularly about pharmaceutical products; orchestrate scams
12	Mariposa botnet	2009 (June)	2009 (Dec 23)	15.5 million bots	Sell parts of the botnet to cybercriminals; install pay-per-install toolbars; sell stolen credentials for online services; launder stolen bank login credentials and credit card details via an international network of money mules; manipulate search engines to serve pop-up ads
13	Mega-D botnet		2009 (Oct 11)	509 thousand bots	Send unsolicited traffic
14	Pushdo A botnet	2007 Revived in 2013 (May)	Multiple attempts (2008, 2009, 2010); still Active	1.5 million bots in10 countries	Deliver financial malware using spamming modules; orchestrate spam campaigns with controllers of other botnets; install framework for other botnets; update infected computers with newer version of malware
15	Rustock botnet (RKRustok, Costrat)	2006 (June)	2008 2011 (March)	1 million bots	Send unsolicited traffic
16	Srizbi botnet (Cbeplay, Exchanger)	2007 (March)	2008 (Nov)	450 thousand bots	Send unsolicited traffic to support political causes
17	Storm botnet	2007 (Jan)	2008	160 thousand bots	Send unsolicited traffic with provocative subject matter
18	Waledac botnet (Waled, Waledpak)	2008	2010 (March)	80 thousand bots	Send unsolicited traffic
19	ZeroAccess botnet (Sirefef)		2013 (6 Dec)	2 million bots	Mine Bitcoins; hijack search results; perpetrate click frauds; direct traffic to selected websites

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

The first part of the model examines how the volume, diversity, duration, and unpredictability of the botnet takedown are influenced by the characteristics of the botnet controller (i.e., the individuals and systems that run the botnet), the characteristics of the takedown initiative, and the efficacy of the legal environment. The second part of the model examines how the characteristics of the takedown attack influence the performance of the botnet takedown initiative (assessed as improvement and collateral damage). The dimensions used to measure botnet takedown performance are consistent with the approach to accelerate takedown process proposed by Nadji and colleagues (2013).

Takedown attack dimensions

1. *Volume:* the number of uninterrupted action events that comprise each takedown initiative. The actions events can be legal (i.e., a court or enforcement authorities are involved), technology (i.e., hardware or software is used), capacity (i.e., the domain of effectiveness of legal or technology actions), promotion (i.e., actions to gather more supports and users' participation for attack initiatives), and service (i.e., required by end users of compromised devices before and after attack)

2. *Diversity:* the extent to which the sequence of actions of a takedown initiative is comprised of actions of many different types. For example, a low-diversity attack initiative would be one where all 10 actions are technology related, where as a high-diversity attack initiative would include actions of many types.

3. *Duration:* the time elapsed from the beginning to the end of the botnet takedown initiative.

4. *Unpredictability:* the extent to which the sequential order of the novel actions in the botnet takedown initiative is dissimilar from previous takedown initiatives on the same botnet or other botnets from the botnet controller's perspective.

Botnet controller characteristics

1. *Motivation:* a statement that explains why the botnet controllers do what they do. Czosseck and colleagues (2011) conclude, "botnets have developed from a subject of curiosity to highly sophisticated instruments for illegally earning money".

2. *Botnet structure:* refers to whether the botnet has a command-and-control infrastructure, a peer-to-peer infrastructure, or a mixture of the two. Most botnets use a command-and-control infrastructure (Nadji et al., 2013), but regardless of what type of network is used to communicate between nodes, when a network of bots is available, they all follow the instructions from a command-and-control server (Freiling et al., 2005).

3. *Past performance:* measured by the size of the botnet. Past studies have employed various definitions of botnet size due to cloning, temporary migration, and hidden structure issues (Abu Rajab et al., 2007).

4. *Time to takedown start:* the time elapsed from when the botnet was first discovered to the time when the botnet takedown initiative is launched.

Takedown initiative characteristics

1. *Organizational heterogeneity:* the diversity of a takedown organization's demographics, knowledge, and experience. Ferrier (2001) suggests that homogeneity results in a persistent and dominant logic and cognitive strategy, but the heterogeneity that comes with different types of demographics, knowledge, and experience enables organizations to generate more complex and unpredictable strategic actions, facilitate better problem sensing, and match complex competitive challenges.

2. *Past performance:* the number of botnets that the members of the initiative have taken down in the past.

3. *Investment:* refers to the investment a takedown organization makes in security measures.

4. *User participation:* the number of users and organizations that need to act to bring the botnet down.

Legal environment efficacy

1. *Botnet takedown order:* the order in which a legal authority gives permission to law enforcement units to shutdown or seize botnet elements. Watters and colleagues (2013) investigated legal activities by the Internet Corporation for Assigned Names and Numbers (ICANN) as one of the tools to prevent botnet attacks and found that ICANN lacks the ability and interest in ensuring data integrity is maintained as a priority. They advocate that ICANN should reform its policies, procedures, and standards to exert influence and authority on registrars.

2. *Mechanisms to prevent benefits from botnets:* examples include approaches focused on scaling and metric values and the "walled garden" technique

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

(i.e., restricting convenient access to non-approved information and applications). In examining scaling and metric values of activities between hosts and resources, Tiirmaa-Klaar and colleagues (2013b) identified various benefits, including effective mitigation of various attacks and activities. However, the techniques also caused extensive damage such as blocking legitimate activities and impacting user acceptance. In examining the walled garden technique, they identified critical side effects because it was not accepted by all customers of internet service providers and led to difficult legal situations. Although some negative impacts were identified, this model highlights how up-to-date and dynamic prevention rules and policies (beyond public awareness) make botnets less attractive and profitable.

3. *Botnet controller prosecution:* empowers the takedown attack and protects the cyberspace from similar attacks and should decrease the duration of takedown attack.

Takedown performance

1. *Improvement:* results from the takedown initiative, such as reducing the volume of spam traffic, reducing the number of data breaches, or reducing the number of infected machines.

2. *Collateral damage:* the number of organizations that were negatively affected due to execution of the botnet takedown initiative.

Hypotheses

The model provides a framework in which to cast important questions and to enhance understanding of what constructs are of principal consequence for positively contributing to botnet takedowns while minimizing collateral damage. Thus, based on this model, several hypotheses can be derived:

Hypothesis 1. *More aggressive legal action is positively correlated with an improvement in takedown performance.* (This hypothesis is tentatively supported by the observation that, with the exception of four botnet takedowns [Pushdo, Kelihos, Lethic and Storm], the majority of the successful takedowns had a significant legal component.)

Hypothesis 2. *More informed legal action and past attack and defense performance reduces collateral damage.*

Hypothesis 3. *Organizational heterogeneity of the takedown initiative is positively correlated with takedown attack unpredictability.* (This hypothesis is analogous to H1a from Ferrier [2001].)

Hypothesis 4. *Takedown attack volume is positively correlated with an improvement in takedown performance.* (This hypothesis is analogous to H5 from Ferrier [2001].)

Hypothesis 5. *Takedown attack duration is positively correlated with an improvement in takedown performance.* (This hypothesis is analogous to H6 from Ferrier [2001].)

Hypothesis 6. *A decentralized botnet structure is negatively correlated with takedown performance and unpredictability.*

Conclusions

In support of enhancing botnet takedown performance, this article has provided two contributions: i) an overview of a preliminary database of botnet takedown initiatives and ii) a theoretical model to help predict the success or failure of future takedown initiatives.

This work is relevant to researchers, policy makers, and industry professionals. In particular, personnel in technical, legal, and management functions of organizations interested can use the suggested model to improve the quality of their communications by using similar taxonomy and accelerate decision making for the purpose of launching and operating botnet takedown initiatives. Also, these findings will be relevant to entrepreneurs who wish to launch and grown cybersecurity ventures that provide solutions to botnet and malware problems.

The preliminary database and proposed model mark the beginning of a potentially fruitful avenue of research. The database needs to be augmented and refined; the model and its associated hypotheses need to be tested. As our knowledge improves, the intention is that the empirical data and the model constructs will evolve and cybersecurity experts will become more efficient in taking down botnets through various means.

Citation: Shirazi, R. 2015. Botnet Takedown Initiatives: A Taxonomy and Performance Model. *Technology Innovation Management Review*, 5(1): 15–20. http://timreview.ca/article/862

Keywords: botnet takedowns, dismantle cybercriminal networks, disrupt online networks, cyber-attacks

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

About the Author

Reza Shirazi is an Analyst Programmer at the Canada Revenue Agency, Information Technology Branch. Previously, he worked for various government departments and the private sector. He holds a BSc in Computer Software Engineering from the Islamic Azad University in Tehran, Iran, and an MEng in Technology Innovation Management from Carleton University in Ottawa, Canada.

References

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. 2006. A Multifaceted Approach to Understanding the Botnet Phenomenon. In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement:* 41–52. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/1177080.1177086

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. 2007. My Botnet is Bigger than Yours (Maybe, Better than Yours): Why Size Estimates Remain Challenging. In *Proceedings of the HotBots '07 First Workshop on Understanding Botnets:* 5. Berkeley, CA: USENIX Association.

Borrett, M., Carter, R., & Wespi, A. 2013. How Is Cyber Threat Evolving and What Do Organizations Need to Consider. *Journal of Business Continuity & Emergency Planning,* 7(2):163–171.

Cremonini, M., & Riccardi, M. 2009. The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization. In *Proceedings of the 2009 European Conference on Computer Network Defense (EC2ND):* 52–54. Washington, DC: IEEE Computer Society.

Czosseck, C., Klein, G., & Leder, F. 2011. On the Arms Race around Botnets: Setting up and Taking down Botnets. In *Proceedings of the 3rd International Conference on Cyber Conflict (ICCC 2011):* 1-14. Washington, DC: IEEE Computer Society.

Dagon, D., Gu, G., Lee, C. P., & Lee, W. 2007. A Taxonomy of Botnet Structures. In *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC 2007):* 325–339. http://dx.doi.org/10.1109/ACSAC.2007.44

Dittrich, D. 2012. So You Want to Take Over a Botnet. In *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET 2012):* 6. Berkeley, CA: USENIX Association.

Feily, M., Shahrestani, A., & Ramadass, S. 2009. A Survey of Botnet and Botnet Detection. In *Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009):* 268–273. Washington, DC: IEEE Computer Society.

Ferrier, W. 2001. Navigating the Competitive Landscape: The Drivers and Consequences of Competitive Aggressiveness. *Academy of Management Journal,* 44(4): 858–877. http://dx.doi.org/10.2307/3069419

Freiling, F. C., Holz, T., & Wicherski, G. 2005. Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks. In *Computer Security: Lecture Notes in Computer Science, 3679:* 319–335. Berlin: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11555827_19

Kok, J., & Kurz, B. 2011. Analysis of the Botnet Ecosystem. In *Proceedings of the 10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE 2011):* 1–10. Berlin: VDE.

Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D. & Lee, W. 2013. Beheading Hydras: Performing Effective Botnet Takedowns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security:* 121–132. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/2508859.2516749

Nappa, A., Fattori, A., Balduzzi, M., Dell'Amico, M., & Cavallaro, L. 2010. Take a Deep Breath: A Stealthy, Resilient and Cost-Effective Botnet Using Skype. In *Detection of Intrusions and Malware, and Vulnerability Assessment: Lecture Notes in Computer Science, 6201:* 81–100. Berlin: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-14215-4_5

Plohmann, D., Gerhards-Padilla, E., & Leder, F. 2011. *Botnets: Detection, Measurement, Disinfection & Defence.* Heraklion, Greece: European Network and Information Security Agency.

Schaffer, G. P. 2006. Worms and Viruses and Botnets, Oh My! Rational Responses to Emerging Internet Threats. *IEEE Security and Privacy,* 4(3): 52–58. http://dx.doi.org/10.1109/MSP.2006.83

Scully, T. 2013. The Cyber Security Threat Stops in the Boardroom. *Journal of Business Continuity & Emergency Planning,* 7(2): 139–147.

Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. 2013a. Botnets, Cybercrime and National Security. In *Botnets:* 1–40. London: Springer. http://dx.doi.org/10.1007/978-1-4471-5216-3_1

Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. 2013b. Botnets: How to Fight the Ever-Growing Threat on a Technical Level. In *Botnets:* 41–97. London: Springer. http://dx.doi.org/10.1007/978-1-4471-5216-3_2

Watters, P. A., Herps, A., Layton, R., & McCombie, S. 2013. ICANN or ICANT: Is WHOIS an Enabler of Cybercrime? In *Proceedings of the Fourth Cybercrime and Trustworthy Computing Workshop (CTC 2013):* 44–49. Washington, DC: IEEE. http://dx.doi.org/10.1109/CTC.2013.13

Whitehouse, S. 2014. Opening Statement. In *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* Washington, DC: U.S. Senate Judiciary Subcommittee on Crime and Terrorism.

Wikipedia. 2014. Botnet. *Wikipedia.* Accessed January 10, 2015: http://en.wikipedia.org/wiki/botnet

Zeidanloo, H. R., Shooshtari, M. J. Z., Amoli, P. V., Safari, M., & Zamani, M. 2010. A Taxonomy of Botnet Detection Techniques. In *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010),* 2: 158–162. Washington, DC: IEEE. http://dx.doi.org/10.1109/ICCSIT.2010.5563555

Zhao, Y., Xie, Y., Yu, F., Ke, Q., Yu, Y., Chen, Y., & Gillum, E. 2009. BotGraph: Large Scale Spamming Botnet Detection. In *Proceedings of the 4th USENIX Symposium on Networked Systems Design & Implementation (NSDI 2009),* 9: 321–334.

Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

> *To know is to control.*
>
> Ishmael Scott Reed
> Poet, essayist, and novelist

Today's vehicles depend on numerous complex software systems, some of which have been developed by suppliers and must be integrated using "glue code" so that they may function together. However, this method of integration often introduces cybersecurity vulnerabilities at the interfaces between electronic systems. In this article we address the "glue code problem" by drawing insights from research on supplier-manufacturer outsourcing relationships in the automotive industry. The glue code problem can be framed as a knowledge coordination problem between manufactures and suppliers. Car manufacturers often employ different levels of intrusiveness in the design of car subsystems by their suppliers: the more control over the supplier the manufacturer exerts in the design of the subsystem, the more intrusive the manufacturer is. We argue that high intrusiveness by car manufacturers in defining module interfaces and subcomponents for suppliers would lead to more secure cars.

Introduction

The modern car is increasingly dependent on electrical and software systems. A modern vehicle has anywhere from 30 to 70 electronic control units that monitor and control its different subsystems (Studnia et al., 2013a), which are integrated using "glue code" (Checkoway et al., 2011). The glue code enables car manufacturers to outsource the development of particular systems and subsystems, which are then integrated when the car is assembled.

However, within and between these modules, several cybersecurity vulnerabilities in the modern car have been identified and documented by researchers. Examples include vulnerabilities in sound systems, Bluetooth modules, onboard diagnostics systems, cellular communications, and the bus connecting electronic control units, (Checkoway et al., 2011; Eichler, 2007; Hoppe et al., 2009; Koscher et al., 2010; Raya & Hubaux, 2007; Wolf et al., 2004). Practitioners have also stressed how vulnerable the modern car is to cyber-attacks (Miller & Valasek, 2013; Venturebeat, 2013; Yadron, 2014). Both local and remote attacks have been documented (Studnia et al., 2013a). Theft, electronic tuning, sabotage, and surveillance are among the goals of those who cyber-attack cars (Studnia et al., 2013a). Most vulnerabilities in the modern car arise from incorrect assumptions made by the glue code that calls functions on different electronic control units (Checkoway et al., 2011). These incorrect assumptions may occur at the subcomponent level as well as the interface level.

Checkoway and colleagues (2011) argue that the true source of the glue code problem can be traced back to the setup of the ecosystems used to manufacture cars. Auto manufacturers build ecosystems to outsource digital systems in the same way that they outsource mechanical parts. Although every supplier tests their modules, security vulnerabilities usually arise when those modules are subsequently integrated by the car manufacturers. Outsourcing module design may introduce security vulnerabilities at the interface between modules and the car (i.e., in the glue code), as well as between distinct modules designed by external suppliers. The latter source of vulnerabilities is caused by feature interaction problems between different modules and this source of vulnerabilities is outside the scope of this article.

Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

By analyzing various security solutions that have been proposed to improve the overall security of the modern car (Bouard et al., 2013; Herrewege, et al., 2011; Studnia et al., 2013a; Stumpf et al., 2009; Wolf & Gendrullis, 2012; Wolf & Weimerskirch, 2004), we observe that the proposed solutions: i) only focus on providing technical architectures of security solutions, ii) would typically require substantial changes to existing implementation processes in the automobile industry, and iii) do not directly address the glue code problem identified by Checkoway and colleagues (2011). To address these shortcomings, we examined literature on manufacturer-supplier relationships. As will be described below, we identified that the manufacturer's level of intrusiveness in supplier design could aid in solving the interface boundary, or glue code, problem. In particular, we argue that, for manufacturers to avoid security vulnerabilities at the boundaries between electronic control units, they should be highly intrusive in the supplier design of the module interfaces and subcomponents that call other electronic control units in the car.

In the following section, we describe the proposed cybersecurity solutions for cars and existing manufacturer-supplier relationships. Next, we examine an existing analytical framework and propose our solution. We close by outlining our contribution and offering conclusions.

Proposed Solutions

Three broad categories of solutions have been proposed by various researchers: i) encryption of communications, ii) anomaly detection, and iii) improved integrity of the embedded software (Studnia et al., 2013a). Table 1 summarizes representative solutions and their salient features.

Car manufacturers have been increasingly outsourcing module design (Calabrese & Erbetta, 2005). Suppliers organize themselves around manufacturers' facilities geographically to form supplier parks (Collins et al., 1997; Larsson, 2002; Volpato, 2004). In addition to geo-

Table 1. Representative cybersecurity solutions for the modern car

Security Solution	Salient Features
Proxy-Based Security Architecture for CE Device Integration (Bouard et al., 2013)	• Proxy-based IP security solution to secure consumer electronic devices able to access a car's onboard network. • Enforces communication decoupling between internal and external networks by using a security proxy. • Approach requires partial redesign of electronic control units to support in-band signaling between the control units and the security proxy.
Multipurpose Electronic control Units and Hardware Security Module (Stumpf et al., 2009; Wolf & Gendrullis, 2012)	• A dedicated hardware security module governs all traffic between electronic control units and authenticates individual frames. • Hardware security module is then implemented in a system that uses the concept of virtualization to centralize all electronic control units in a car onto a single virtual machine • Integrates inherent features of virtual machines: integrity, trustworthiness, and authenticity.
Security in Automotive Bus Systems (Wolf et al., 2004)	• Secure the existing in-car network using controller authentication, encrypted communication and gateway firewalls. • Inter Bus communication happens through a central authentication and encryption gateway on each bus.
CANAuth (Herrewege et al., 2011)	• Backward-compatible controller area network (CAN) authentication protocol designed using hashed message authentication code (HMAC). • This protocol uses the existing CAN bus and forms an additional layer on top of the existing protocol.
Intrusion Detection System (Studnia et al., 2013b)	• Automotive security using an intrusion detection system for the CAN bus.

Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

graphic allocation, smaller suppliers usually form a hierarchy behind large first-tier suppliers forming around car manufacturers (Volpato, 2004). Knowledge and task partitioning differ depending on the relationships between supplier and manufacturer (Cabigiosu et al., 2013; Zirpoli & Camuffo, 2009) as well as the nature of the product being co-developed (Takeishi, 2002). Manufacturers and suppliers co-develop modules with varying levels of intrusion by the manufacturer in the supplier design (Cabigiosu et al., 2013).

The Manufacturer-Supplier Co-Development Approach

Cabigiosu and colleagues (2013) compared two similar vehicle component co-development projects carried out by the same first-tier supplier with two different automakers. They used an analytical framework to analyze the manufacturer's approach to supplier integration in product development. The results showed that the two manufacturers employed different levels of "intrusiveness" in supplier design. Manufacturer intrusiveness represents the level of detail and the amount of coordination the manufacturer employed in defining the design of the respective artifact. An intrusive approach to the co-development is an approach where the manufacturer exerts high level of control over the supplier's design decisions. The level of intrusiveness influences the knowledge the manufacturer has about the interface and the subcomponents of the module. Analyzing the two different approaches reported by Cabigiosu and colleagues (2013), and the corresponding degrees of intrusiveness with each approach, leads to insights on how the glue code problem may arise and what car manufacturers can do to prevent it.

According to Cabigiosu and colleagues (2013), manufacturers engage with suppliers at different levels of intrusiveness in:

1. *Module-to-car system-level design:* includes functional and performance parameters that the module has to adhere to in order for it to comply with overall functional and performance parameters of the car as a whole.

2. *Module-to-module interface design*: includes protocol-level functionality that the module has to adhere to in order for it to interoperate with various other modules in the car.

3. *Individual-subcomponent-to-module system-level design:* includes functional and performance parameters that various subcomponents in the module have to adhere to for the module to work as a whole.

4. *Individual subcomponents design:* functional- and protocol-level parameters that subcomponents have to adhere to.

Table 2 compares the approaches taken by two manufacturers in co-developing an air conditioning system with the same supplier (Cabigiosu et al., 2013). Manufacturer A's approach can be characterized as intrusive whereas manufacturer B's approach can be characterized as non-intrusive.

Table 2. Comparison between intrusive and non-intrusive approaches to manufacturer-supplier co-development (Cabigiosu et al., 2013)

	Manufacturer A's Approach (Intrusive)	**Manufacturer B's Approach (Non-Intrusive)**
Interface definition	• Stable and detailed • Definitions frozen before design starts • Specifics are clear, easy to follow, and do not change	• Fluid and changing • Set the main concept and architecture but allow supplier to suggest design
Co-development approach	• Formal information-sharing sessions monthly and bi-weekly • Daily communications, sometimes face to face • Mainly to sort out component interdependencies	• Heavily outsourced engineering tasks to supplier. • Used a standard codified co-development practice • Used rigid systems and procedures
Knowledge partitioning	• Owned component-specific knowledge	• Did not own component-specific knowledge

Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

The glue code problem can be seen as a knowledge coordination problem. Suppliers design components based on performance and functional specifications provided by the manufacturer. Design decisions can sometimes be left to the discretion of the supplier, who may assume that particular components in the car work in certain ways. This was the case with the Airbiquity software component analyzed by Checkoway and colleagues (2011), where they found that the code calling this component and binding it to other telematics functions made the wrong assumptions about the component supported packet size and resulted in a buffer overflow vulnerability. Packet sizes are usually defined as part of the interfaces; given that the car manufacturer did not know the right packet size used by the software component shows that the manufacturer was non-intrusive in defining this interface. An intrusive strategy would avoid such a problem because the manufacturer would know the right packet size because it was the one defining it. Only the manufacturer is in a position that would allow a holistic view of all the different electronic control units and their inner workings. Thus, the glue code problem can be reduced if the manufacturer employs the right level of intrusiveness with different suppliers. We argue that the right level of intrusiveness by a manufacturer for avoiding the glue code problem is being highly intrusive in defining the module interfaces and the inner subcomponents of the electronic control unit module that call other modules in the car. This degree of intrusiveness in the manufacturer-supplier relationship is similar to a hybrid-control governance model of open source platforms (Noori & Weiss, 2013), where increased control yields higher quality but does require greater effort in the form of overseeing all the parties involved. Where increased quality equates to increased security, this added effort will be worthwhile.

Conclusion

As described earlier, security solutions can by broadly divided into three main categories: i) encryption of communications, ii) anomaly detection, and iii) integrity of the embedded software, where the final category refers to approaches that ensure the car's critical software is not affected by a cyber-attack (Studnia et al., 2013). Our contribution adds to this third category by identifying the manufacturer-supplier relationship that reduces the risk of vulnerabilities at the boundaries between electronic control units and thus protects the integrity of the car's critical software modules.

Our contribution allows car manufacturers to employ the right level of intrusiveness in their supplier design to increase the level of cybersecurity in their cars. It allows individuals responsible for leading engineering efforts at both manufacturer and supplier organizations and individuals controlling manufacturer-supplier inter-firm relations to pick the right working model for building secure cars. We encourage the research community to further explore manufacturer-supplier relationship theory and other managerial theories in their search for a solution to securing the car.

Manufacturers can choose the optimal degree of intrusiveness when co-developing new products with their suppliers. We argue that an intrusive strategy can be employed by manufacturers when developing electronic control units to reduce the risk of cybersecurity vulnerabilities at the boundaries between systems. We invite further research into this domain to tackle the cybersecurity problems of the modern car. Future work could empirically test our claim that increased manufacturer intrusiveness in supplier design leads to more secure cars.

About the Authors

Mohamed Amin is an MASc student in the Technology Innovation Management program at Carleton University in Ottawa, Canada. His research interests include cybersecurity, API strategy, and industry architecture. He works as a Solution Architect for Alcatel-Lucent Canada, where he designs and delivers network solutions for various internet service providers around the world.

Zaid Tariq is completing his MEng in Technology Innovation Management at Carleton University in Ottawa, Canada. He also holds a BEng degree in Computer Engineering from McGill University in Montreal, Canada. He is a Senior Network Engineer at Cisco Systems and has 9 years experience working in the network design, architecture, and test domains.

Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

References

Bouard, A., Schanda, J., Herrscher, D., & Eckert, C. 2013. Automotive Proxy-Based Security Architecture for CE Device Integration. In P. Bellavista, C. Borcea, C. Giannelli, T. Magedanz, & F. Schreiner (Eds.), *Mobile Wireless Middleware, Operating Systems, and Applications:* 62–76. Berlin: Springer Berlin Heidelberg.

Cabigiosu, A., Zirpoli, F., & Camuffo, A. 2013. Modularity, Interfaces Definition and the Integration of External Sources of Innovation in the Automotive Industry. *Research Policy,* 42(3): 662–675. http://dx.doi.org/10.1016/j.respol.2012.09.002

Calabrese, G., & Erbetta, F. 2005. *Outsourcing and Firm Performance: Evidence from Italian Automotive Suppliers.* Paper presented at the 13th Annual IPSERA Conference. Catania: Universita di Catania.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Patel, S., Roesner, F., Czeskis, A., & Kohno, T. 2011. *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* Paper presented at the USENIX Security Symposium. San Francisco: USENIX Association.

Collins, R., Kimberly, B., & Pires, S. 1997. Outsourcing in the Automotive Industry: From JIT to Modular Consortia. *European Management Journal, 15(5):* 498–508. http://dx.doi.org/10.1016/S0263-2373(97)00030-3

Eichler, S. 2007. A Security Architecture Concept for Vehicular Network Nodes. In *Proceedings of the 6th International IEEE Conference on Information, Communications & Signal Processing:* 1–5. Washington, DC: IEEE. http://dx.doi.org/10.1109/ICICS.2007.4449730

Herrewege, A., Singelee, D., & Verbauwhede, I. 2011. *CANAuth: A Simple, Backward Compatible Broadcast Authentication Protocol for CAN Bus.* Paper presented at the ECRYPT Workshop on Lightweight Cryptography. Louvain-la-Neuve, Belgium: ECRYPT.

Hoppe, T., Kiltz, S., & Dittmann, J. 2009. Automotive IT Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats. In *Computer Safety, Reliability, and Security – Lecture Notes in Computer Science, 5575:* 145–158. Berlin: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-04468-7_13

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., & Savage, S. 2010. Experimental Security Analysis of a Modern Automobile. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy:* 447–462. Oakland, CA: IEEE.

Larsson, A. 2002. The Development and Regional Significance of the Automotive Industry: Supplier Parks in Western Europe. *International Journal of Urban and Regional Research,* 26(4): 767–84. http://dx.doi.org/10.1111/1468-2427.00417

Miller, C., & Valasek, C. 2013. *Adventures in Automotive Networks and Control Units.* Paper presented at DEF CON 21 Hacking Conference. Las Vegas, NV: DEF CON.

Noori, N., & Weiss, M. 2013. Going Open: Does it Mean Giving Away Control? *Technology Innovation Management Review,* 3(1): 27-31. http://timreview.ca/article/647

Raya, M., & Hubaux, J. P. 2007. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security,* 15(1): 39–68.

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Laarouchi, Y. 2013a. A Survey of Security Threats and Protection Mechanisms in Embedded Automotive Networks. In *Proceedings of the 2nd Workshop on Open Resilient Human-Aware Cyber-Physical Systems (WORCS-2013).* Budapest, Hungary: IEEE. http://dx.doi.org/10.1109/DSNW.2013.6615528

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Laarouchi, Y. 2013b. Security of Embedded Automotive Networks: State of the Art and a Research Proposal. In *Proceedings of 2nd Workshop on Critical Automotive Applications: Robustness & Safety of the 32nd International Conference on Computer Safety, Reliability and Security.* Toulouse, France: SAFECOMP.

Stumpf, F., Meves, C., Weyl, B., & Wolf, M. 2011. *A Security Architecture for Multipurpose ECUs in Vehicles.* Paper presented at the 25th Joint VDI/VW Automotive Security Conference. Ingolstadt, Germany.

Takeishi, A. 2002. Knowledge Partitioning in the Interfirm Division of Labor: The Case of Automotive Product Development. *Organization Science,* 13(3): 321–338. http://dx.doi.org/10.1287/orsc.13.3.321.2779

VentureBeat. 2013. Ford Wants You to Join It in Hacking Car Software and Hardware. *VentureBeat.* Accessed January 10, 2015: http://venturebeat.com/2013/11/06/ford-wants-you-to-join-it-in-hacking-car-software-and-hardware-video/

Volpato, G. 2004. The OEM-FTS Relationship in Automotive Industry. *International Journal of Automotive Technology and Management,* 4(2/3): 166–197. http://dx.doi.org/10.1504/IJATM.2004.005325

Weimerskirch, A. 2012. *Automotive and Industrial Data Security.* Paper presented at the Cybersecurity for Cyber-Physical Systems Workshop. Ann Arbor, MI: National Institute of Standards and Technology.

Wolf, M., & Gendrullis, T. 2012. Design, Implementation, and Evaluation of a Vehicular Hardware Security Module. In H. Kim (Ed.), *Information Security and Cryptology-ICISC:* 302–318. Berlin: Springer Berlin Heidelberg.

Wolf, M., Weimerskirch, A., & Paar, C. 2004. *Security in Automotive Bus Systems.* Paper presented at Workshop on Embedded Security in Cars (ESCAR 2004). Bochum, Germany: ESCAR.

Yadron, D. 2014. Tesla Invites Hackers for a Spin. *The Wall Street Journal Blog.* Accessed January 10, 2015: http://blogs.wsj.com/digits/2014/08/08/telsa-invites-hackers-for-a-spin/

Zirpoli, F., & Camuffo, A. 2009. Product Architecture, Inter-Firm Vertical Coordination and Knowledge Partitioning in the Auto Industry. *European Management Review,* 6(4): 250–264. http://dx.doi.org/10.1057/emr.2009.25

Citation: Amin, M., & Tariq, Z. 2015. Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities. *Technology Innovation Management Review,* 5(1): 21–25. http://timreview.ca/article/863

Keywords: cybersecurity, vulnerabilities, automobile manufacturing, car design, supplier, outsourcing, control, governance, supplier-manufacturer relationships, glue code, intrusiveness

Identifying the Challenges in Commercializing High Technology: A Case Study of Quantum Key Distribution Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

> *"It is time for us all to stand and cheer for the doer, the achiever – the one who recognizes the challenges and does something about it."*
>
> Vince Lombardi (1913–1970)
> Player, coach, and executive of American Football

This article examines the challenges in commercializing high technologies successfully and sustainably using quantum key distribution (QKD) technology as a case study. Quantum communication is increasingly relevant to cybersecurity and nanotechnology, which will replace current technologies and change the way we live. To understand how such high technology could be successfully commercialized, we interviewed individuals from four metrology institutions and two international companies. The result revealed that scattered and small markets, supply chain development, technology validation/certification, a lack of available or adequate infrastructure, and after-sales services are the most serious challenges facing successful commercialization of quantum communication technology. To validate these challenges, we conducted a survey of 60 experts, 49 of whom agreed that above-mentioned factors could affect the commercialization success of QKD technology. Likewise, the survey revealed that technical development, customer orientation/awareness, and government regulations could also hinder the commercialization of QKD technology.

Introduction

One of the key drivers for economic growth nowadays is knowledge, and it involves high investment in education and training, research and development (R&D), and relationships between governments, academia, and industry (Lowe, 2005). To realize the benefits of knowledge and to receive returns from these investments, the resulting innovations or inventions must be sold, or commercialized (Meyers, 2009). Indeed, commercialization is an important contributor to economic growth (Tahvanainen & Nikulainen, 2011), and it makes technology available to end users. In essence, commercialization is an exchange of know-how for money (Speser, 2008), but it can be perceived in different ways, including:

- a series of activities for converting an invention to a product or service (Rosa & Rose, 2007)
- the process of taking the R&D of an organization to an industry (Cornford, 2002)
- the identification of a business opportunity for a certain scientific or engineering invention and subsequent steps to design, develop, and manufacture the invention to make it useful (Michael, 1990)
- the adoption of a new technology or service by customers (Tanev & Frederiksen, 2014)
- any scheme that permits members of a technological innovation team to receive economic gains from their

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

efforts, including through patent licensing, research grants, and R&D joint ventures (Kalaitzandonakes, 1997)

Here, we focus on the definition of Pellikka and Malinen (2011) who state that commercialization brings high-technology innovations to the market and makes innovative products benefit of society. Commercialization is not a straightforward process; many challenges must be overcome. Although previous studies have outlined some challenges, this study also attempts to fill the perceived gap by identifying additional challenges of commercialization, particularly for high technologies. Usually, new technologies face many problems in the beginning of their lifecycle because they are new to the end users and they lack standardization or third-party certification. In this study, we examine quantum key distribution (QKD) technology as a case study because is a new high technology of increasing importance within the domain of cybersecurity.

QKD is a mean of sending and receiving safe information; it uses cryptographic keys to encode information at the point of dispatching and the keys are used by the receiver to decode or retrieve the information. Presently, QKD kits are commercially available but there are no any independent measurements and standards in the industry. Due to cybersecurity pressures, the European Union has funded a project named "Metrology for Industrial Quantum Communications" (MIQC). The MIQC project aims to develop and commercialize standards for the QKD technology systems. Most of the leading metrology centers in Europe participated in the development of new QKD standards and certification. However, in this article, we present the findings of the commercialization study, which examined how the new QKD technology would be available in the market. Although the case study focuses on QKD technology, the main motive for sharing the findings is that we believe that the study has broader implications and value for assisting researchers and innovators/inventors in many high-technology fields; the findings may help them become aware of and overcome hidden commercialization challenges.

This article is structured as follows. First, we review the literature on the challenges of commercializing high technology. Next, we describe the interview and survey methodology used in our QKD case study and then we present the results. Finally, we discuss the key findings and provide conclusions.

Literature Review: Commercializing High Technology

For a high-technology innovation to successfully reach the market, a company's commercialization team must identify, obtain, combine, and manage needed technological knowledge. The innovation must be developed into a product, which must then be manufactured, marketed, and distributed. Ongoing success with subsequent commercialization attempts can be facilitated by a growth strategy that exploits economies of joint costs and scale. Furthermore, an innovation can be successful if the innovation team or company can adhere to their learning paths and create and maintain a good network (Chandler, 2005). Additionally, the team must not only concentrate on a niche market but also focus on a wider (potential) market because a niche market may not be able to sustain the product in long run (Slater & Mohr, 2006).

Likewise, to successfully commercialize high technology, it is necessary to follow a market-oriented process: one that starts with market, ends with the market, and involves the market throughout the entire process (Valiauga, 2013). Nichols (2013) adds that commercialization is supposed to be a well-planned and well-implemented activity that improves product performance relative to its price and that focuses on competitors. Fletcher and Bourne (2012) state that there are 10 simple rules for successful commercialization: i) science must be differentiated from business; ii) know that there is no one specific way to commercialize; iii) know the company's rights and the rights of its partners, iv) consider the of implications of private and public business; v) decide what the company wants to give; vi) be realistic; vii) accept that a market may not exist in the beginning; viii) consider the difference between wants and needs; ix) make the invention comprehensive; and x) customers are the ultimate peer reviewers.

Pellikka and colleagues (2012) argue that the main difficulties of the commercialization process relate to marketing, resources, the business environment, and the planning and management of commercialization process. The marketing challenges relate to a failure to obtain sufficient and relevant market information, a failure to use it properly, insufficient knowledge about the international market and the business growth, and an inability to establish both local and international sales and distributions. These scholars explain further that the resource challenges of the commercialization process are an inability to acquire and assign resources,

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

inadequate managerial and business skills, and insufficient funds to market the new product. In the business environment, they identify additional commercialization challenges, including a lack of available or adequate business infrastructure, low market potential, and insufficient business partners. Lastly, these authors mention that lack of a systematic model, time and materials for getting public funds, and insufficient know-how threaten the planning and management of a commercialization process. However, these problems can be overcome through the effective pre-planning activities, better utilization of resources, and internal commercialization training of key staff.

Epting, Gatling, and Zimmer (2011) highlight common challenges with financing, production, distributing and marketing. The authors explain further that many innovators face the following problems in their commercialization adventures:

1. Undue delay caused by the inventor's attempts to "perfect" their product may allow a competitive, lower-quality product to enter the market, to the detriment of the inventor.

2. Licensing manufacturing to another company may hasten market entry, but at the expense of the inventor's control.

3. Funding may be exhausted in pre-sales activities.

4. Distribution and supply chains take time and expertise to establish.

In addition, Parker and Mainelli (2001) identify frequent mistakes made during technology commercialization, including: i) assuming that new features will be beneficial, ii) using top-down market analysis, iii) insufficient testing of the technology, iv) failure to assign a specific person or team to oversee the commercialization process, and v) an inability to value the new technology fully. Rosa and Rose (2007) add that financial problems due to insufficient funds to complete commercialization and human resource problems in the form of a lack of skilful people to sell and promote the innovating products are key obstacles facing technology commercialization.

Tahvanainen and Nikulainen (2011) found that a lack of time and interest, a negative attitude in the research environment, economic risks, conflicts of interest, bureaucratic disturbance, lack of business or commercialization knowledge, incompatibility of commercialization with the ethics of science, and issues with ownership rights are challenges confronting commercialization. Similarly, Bulsara, Gandhi, and Porey (2010) outline difficulties with patent filing processes, commercialization interests, commercialization option selection, commercialization supports, obsolescence of technology, educational and business background of innovator, and the general business environment.

The above scholars hold a wide range of views regarding the challenges of commercialization. Others have identified specific challenges in particular industries. For instance, in focusing on commercialization bio-pharmaceutical knowledge in Iran, Nassiri-Koopaei and colleagues (2014) outline three main obstacles to commercialization in that country and industry: i) policy, ii) regulations, and iii) management. Likewise, Szuhaj and McCullough (2009) argue that supply chain management in the bio-pharmaceutical industry is a particularly critical aspect of commercialization in that industry.

Kaarela (2013), focusing on the nanotechnology, explains that the main processes of commercialization process are market validation in the planning phase and multidisciplinary team and mainstream customers in the execution phase. Although the author focuses on 64 cases in the Finnish-Russian nanotechnology commercialization alliance, he presents many problems associated with the technology commercialization. He notes that most of these challenges come from the business side rather than technology side. He also presents three main challenges: i) understanding the customer needs, ii) describing the business benefits not the technology benefits, and iii) complementing the team's skill with the right partner. In the same view, McNeil and colleagues (2007) list, in their final report for the Technology Administration agency of the United States Department of Commerce, the following barriers to commercialization in the nanotechnology industry: i) the ten-year cycle time from scientific results in a laboratory to a commercial product; ii) the difference between researchers and applied scientists; iii) the difference in funding between basic research and applied research; iv) a lack of understanding that for every dollar invested in basic research almost $100 is required for a commercially viable product; v) long timescales needed for patenting; vi) uncertainty of potential regulations, and vii) the high risk of new scientific results. In addition, Pfautsch (2007) identifies the main barriers to commercialization efforts with carbon nanotube composites: i) the high cost of equipment, ii) a lack of knowledge about environment health and safety, iii) a lack of

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

a risk assessment or lifecycle assessment, iv) a lack of standards, v) a need for properly trained workers, and vi) cross-patenting.

Boehlje (2004) analyzed previous work on commercialization of agricultural technologies and found common challenges that included gaining customer/consumer acceptance, capital market accessibility, value capture/sharing, protecting intellectual property, and selecting innovation strategies.

In the health sector, Booz Allen Hamilton and three other organizations in the United States (2012) confirmed that the problems facing new invention commercialization are access to capital, potential limitations of traditional technology transfer, the need for entrepreneurial skills, and the difficulty of navigating the complexities of the healthcare market. Additionally, Scanlon and Lieberman (2007) analyzed historical medical breakthroughs and found that the two major challenges of commercialization in the medical field are the ability of the academic community to change the culture of the scientists to commercialize their technology and the ability of the business community to communicate successfully with the scientists.

Furthermore, O'Brien and colleagues (2004) investigated barriers to the deployment of integrated gasification combined cycle (IGCC) technology, the most successful method of producing electric power utilizing coal gasification in the US electric industry. They found that the most substantial barriers were financial, environmental, cultural, and legal. The financial barrier consisted of tax issues, credit concerns, project finance, market for emissions credits, licensing fees, and cost of operation. The environmental barrier included emission limitation, environmental permitting processes, and uncertain environmental rules and enforcement. The cultural barriers were regulator viewpoints, public perception, corporate culture of plant developers, past failures, and difficulties of IGCC plants. And, the legal barrier included plant-siting procedures, standard market design, electric industry restructuring, and uncertainty over regulatory treatment.

Although the above-mentioned scholars investigated the same topic in different fields, their findings are summarized in Table 1.

Notably, Table 1 highlights that market- and funding-related issues are the most common challenges in all aforementioned sectors. Our recent research (Al Natsheh et al., 2015) also revealed that the following factors need to be considered during technology commercialization:

- novelty and clear added value
- technology functionality
- a non-complicated first set of products
- product certification/accreditation
- the right team
- sufficient capital
- a good business model
- a proper manufacturing plan
- ongoing updates and product maintenance

Although our recent work focused on university technology transfer, these findings may be applicable to the commercialization of any technology. To reach the source of problems facing the commercialization of high technology, we conducted the present study using QKD technology as a case study. Our goal for the QKD study was to understand how the technology could be successfully commercialized. Before presenting the results, the next section describes our research methodology.

Methodology

To maximize the efficiency and methodological self-consistency of the qualitative method, we followed the guidelines stated by Creswell (2009) and Yin (1994). We used a qualitative research method featuring six interviews with innovators (4) from metrology institutions and individuals from companies (2) engaging in QKD technology, and a survey of stakeholders. Our primary research question was:

> *What are the challenges that can hinder successful commercialization of QKD technology?*

Based on our experience in QKD research projects and other high-technology commercialization projects, we identified five possible challenges that could hinder successful commercialization of QKD technology. They are:

1. Market size
2. Possibility of building the supply chain
3. Availability of technology validation/certification
4. Availability of infrastructure for the new technology
5. Possibility of offering after sales-sales services (especially product update and maintenance)

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

Table 1. Summary of commercialization challenges

Study	Challenges	Application
Pellikka et al. (2012)	Marketing, resources, business environment, and planning and management of commercialization process	General
Tahvanainen & Nikulainen (2011)	Lack of time, lack of interest, negative attitude of research environment, economic risks, conflicts of interest, bureaucratic disturbance, lack of business or commercialization knowledge, incompatibility of commercialization with the ethics of science, and ownership right problem	General
Chiesa & Frattini (2011)	Volatility, interconnectedness, and proliferation of new technologies to fit the market	General
Bulsara et al. (2010)	Patent filing processes, commercialization interest, selecting of commercialization options, commercialization supports, obsolescence of technology, educational and business background of innovator, and general business environment	General
Epting et al. (2011)	Inventor's procrastination for making a perfect product, licensing issues, insufficient funds, and insufficient time and expertise to establish distribution and supply chains	General
Rosa & Rose (2007)	Financial problems and human resource problems	General
Parker & Mainelli (2001)	Innovators' assumption, top-down market analysis, insufficient test of the technology, failure to assign specific person or team to oversee commercialization process and inability to value the new technology	General
Nassiri-Koopaei et al. (2014)	Policy, regulations, and management	Bio-pharmaceutical
Szuhaj & McCullough (2009)	Supply chain management	Bio-pharmaceutical
Kaarela (2013)	Not understanding customer needs, describing technology benefits instead of business benefits, and not complementing team's skill with the right partner	Nanotechnology
McNeil et al. (2007)	Ten-year cycle for innovation, the gap between researcher and applied scientists, the gap in funding between basic research and applied research, lack of understanding that for every dollar invested in basic research almost $100 is required for a commercially viable product, time to patent, uncertainty of potential regulations, and the high risk of new scientific results	Nanotechnology
Pfautsch (2007)	High cost of equipment, lack of knowledge about environment health and safety, lack of a risk assessment or lifecycle assessment, lack of standards, need for properly trained workers, and the issue of cross-patenting	Nanotechnology
Boehlje (2004)	Gaining customer/consumer acceptance, capital market accessibility, value capture/sharing, protecting of intellectual property, and selection of innovation strategy	Food and Agriculture
Booz Allen Hamilton et al. (2012)	Access to capital, potential limitations of traditional technology transfer, the need for entrepreneurial skills, and the difficulty of navigating the complexities of the healthcare market	Health
Scanlon & Lieberman (2007)	Ability of the academic community to change the scientific culture to commercialize technology, and the ability of the business community to communicate successfully with the scientists	Health (Medical)
O'Brien et al. (2004)	Financial, environmental, cultural, and legal	Electricity

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

Interview methodology

The interview questions consisted of three parts. The first part focused on the interviewee's background, especially as it related to previous projects. The second part centralized on the commercialization of QKD technology. The last part focused on the interviewee's general opinions on the commercialization of high technology. Several weeks prior to the interviews, we sent the interview questions to the participants so that they would have prior knowledge about our goals of the study. The interviews for innovators were conducted in Italy and Finland. The average duration of their interviews was 1 hour and all interviews were recorded.

The innovators work with metrology institutions in the United Kingdom, Italy, and Finland. Three of them hold PhD degrees; the fourth holds an MSc degree. Each of them has more than 15 years' experience in the field, and they have participated in several basic and applied research studies. Three of the innovators hold patents; one has developed a few products. At the time of the interviews, they were all working on different innovation projects.

The individuals from the companies are all hold managerial roles. The first participating company was established 10 years ago. It designs and produces single-photon counting avalanche diodes and develops active-quenching integrated circuits. The company has networks in five continents and its products are applied in biomedical, industrial, and astrophysical domains. The second company was founded 11 years ago. Its products provide network encryption and photon counting.

The collected data were analyzed using the method of Miles and Huberman (1994), which includes summarization and extraction of key points. Therefore, we first transcribed the interviews and then summarized them. After that, we pinpointed the main information from the summaries. Thereafter, our qualitative results were derived.

Survey methodology

As a part of the MIQC project, the commercialization team conducted a survey on the project stakeholders' satisfaction and the team included commercialization questions designed to test the qualitative results from the interviews. In the survey, there were 22 questions but five of them were focused on commercialization. The answers were in multiple-choice format, but respondents were allowed to state their reason for either agreeing or disagreeing. Our survey questions were:

1. Do you think that the market size of quantum cryptography can affect its commercial implementation?

2. How important is the development of standards and quality assurances related to the commercial QKD system in order to ensure the commercial success of this technology?

3. How important is the development of a metrological infrastructure for characterizing the optical components of QKD systems in relation to the development of standards for the market take-up of the QKD technology?

4. In your opinion, what do you think can hinder commercial implementation of quantum cryptography?

5. An empirical study on the commercial implementation of quantum cryptography revealed that building of supply chain, technology validation/certification, a lack of available or adequate infrastructure, and after-sales services are the most serious challenges facing successful commercialization of quantum cryptography. Do you agree?

The questions aimed to validate our findings because the intended participants of the survey are QKD professionals. Invitations to participate in the MIQC survey were sent to about 100 people who we considered the necessary stakeholders of quantum communication technology in Europe; 60 of these professionals participated in the survey, which was made available online from the 1st and 30th of September, 2014. Table 2 provides an overview of the survey participants.

Analysis

In this study, we used both qualitative methods (i.e., summarization and extraction of key points from interview data) and quantitative methods (i.e., descriptive statistics from survey data), which allowed the findings to be triangulated. Triangulation combines both qualitative and quantitative research methods to obtain various points of view as well as to validate specific claims; it enables researchers to obtain deep understanding and wide knowledge of a phenomenon (Olsen, 2004; Zawawi, 2007). Our research and triangulation process is summarized in Figure 1.

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

Table 2. Backgrounds and experience levels of the 60 QKD survey participants

	Categories	Number of Participants
Organization	Small and Medium Enterprise (SME)	9
	Public Liability Company (PLC)	1
	University	24
	Governmental Research Institute/Centre	23
	Private Research Institute/Centre	2
	Other: Standard Institute	1
Position	Student	6
	Researcher	35
	Professor	8
	Research and development manager	6
	Senior manager or CEO	5
Experience Level	Under 5 years	13
	5-10 years	22
	11- 15 years	14
	16-20 years	9
	Above 20 years	2

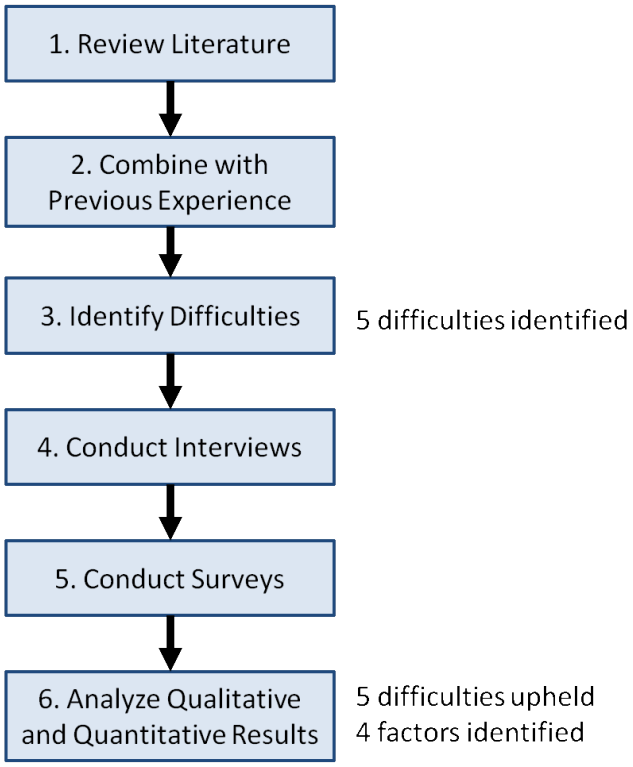

Figure 1. Research process

Findings

Our qualitative data analysis revealed that the critical challenges in commercializing QKD technologies were: i) small market size and distribution channels; ii) building a supply chain; iii) technology validation or certification; iv) a lack of available or adequate infrastructure; and v) after-sales services such as product updates and maintenance. Each of these challenges is briefly described below.

1. *Scattered and small market size:* Our interviewees said that developing an invention was not as difficult as developing a market, especially for the high-technology products. They stressed that the initial market for a new technology is often small, and it might take several years before a large market could be developed. In view of this challenge, there are other problems relating to profitability and sustainability. Our study also revealed that the small-market challenge becomes greater if the small market is scattered geographically, particularly because of higher costs for sales and after-sales services.

2. *Building of supply chain:* Our interviewees pointed out the difficulty of building a supply chain for a new technology. One of reasons they cited was the newness of the technology to both suppliers and consumers. They explained further that the components of the new technology may not actually exist or the existing product may need modifications before they can be used as components; in either case, it can be difficult to find the right suppliers. Similarly, they stressed that finding the right distribution channel may be a serious challenge. They explained that the small market size complicates distribution in terms accessibility to customers. Nonetheless, we found that the most difficult challenge is the identification

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

and development of the right supply chain because the new technology might have several application areas that cannot be supported by existing supply chains.

3. *Technology validation or certification:* Our interviewees re-confirmed one of our findings in the previous studies (Al Natsheh et al., 2015). They said that validation/certification of a new technology is a challenge facing high-technology commercialization. To be certified, a technology must work properly, be of sufficient quality, and be safe to use. However, new technology usually requires new formal testing procedures, which may be expensive and may require several sub-projects. In addition, new standards will prescribe measurements that will most likely require development by the metrology community, given that existing measurements and reference artefacts will not be adequate. Thus, validation/certification appears to be a barrier to high-technology commercialization, because the standards and metrology needed to validate/certify such systems is expensive to develop.

4. *Lack of available or adequate infrastructure:* Our participants mentioned that, in some cases, there is no infrastructure to support new QKD technology. Three interview subjects quickly cited example of 3G Internet connectivity for smartphones. These participants illustrated that, if smartphone technology were developed without any Internet connectivity infrastructure to support it; then, consumers would not be able to use smartphones. One of the participants cited the example of cloud computing, which is now leading the new technologies: if cloud computing were not available, the insurgency of mobile phone applications and other related technologies would not be possible. Therefore all interviewees agreed that a lack of available or adequate infrastructure is a key challenge in the commercialization of high technology.

5. *After-sales services:* Our participants also identified after-sales services as a key challenge facing high-technology commercialization. They explained that selling high-technology products can be less challenging than providing the necessary services to maintain the technology. To confirm another finding from our earlier work (Al Natsheh et al., 2015), we asked the interviewees about the challenges of updating and maintaining products. All of them agreed that it is an important factor to be considered during the technology commercialization process because it also serves as a bottleneck. In support of above-mentioned challenges, the case study technology (i.e., quantum key distribution) requires metrological infrastructure for optical components of quantum optical communication systems, especially for internal single optical components such as single-photon sources and single-photon detectors. A metrology system is mainly for certification and accreditation purposes. Without such a system, quality assurance is at risk. The system level needs to be validated, but validating/certifying techniques are expensive and only yield returns on investment over the long term due to the currently limited market and time-consuming development. Therefore, the aforementioned challenges are apparently evident in the commercialization of QKD technology.

In addition, our quantitative results show that 85% of the QKD professionals we surveyed agreed that market size would affect the successful commercialization of the new QKD technology and the development of standards or quality assurance is necessary for the commercial success of such technology. Forty-nine of the survey participants (82%) agreed that it is essential to have sufficient infrastructure for the new QKD technology in order to make a successful product. Likewise, 49 participants (82%) confirmed that market size, building a supply chain, technology validation/certification, a lack of available or adequate infrastructure, and after-sales services are the most serious challenges facing successful commercialization of QKD. One of the respondents emphasized that: "Customers perceive no urgent need to switch. That's the only problem."

Furthermore, the survey results also revealed that customer orientation/awareness, technical development, and government regulations could affect the commercialization. The reason why many respondents agreed that customer orientation/awareness could hinder QKD commercialization is that QKD deals with industrial systems in which many end users/final customers may not be aware of its importance in the beginning. Table 3 summarizes the quantitative results.

Discussion and Conclusion

Tanev and Frederiksen (2014), Kaarela (2013), Pellikka and colleagues (2012), Chiesa and Frattini (2011), Boehlje (2004), and Parker and Mainelli (2001) found that market-related issues were among the challenges facing technology commercialization. In the same view, our study revealed that scattered and small market size is one of the factors hinder successful commercializa-

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

Table 3. Summary of survey results

Research Statement	Research Question	Positive Response Percentage
1. Market size can affect QKD commercialization	Do you think that the market size of quantum cryptography can affect its commercial implementation?	85%
2. Development of standards and quality assurances are important for QKD commercialization	How important is the development of standards and quality assurances related to the commercial QKD system in order to ensure the commercial success of this technology?	93 %
3. Development of a metrological infrastructure	How important is the development of a metrological infrastructure for characterizing the optical components of QKD systems in relation to the development of standards for the market take-up of the QKD technology?	82 %
4. Market size, building a supply chain, technology validation/certification, lack of available or adequate infrastructure, and after-sales services are the main challenges.	An empirical study on the commercial implementation of quantum cryptography identified the most serious challenges facing successful commercialization of quantum cryptography. Do you agree with the challenges?	82 %

tion of QKD technology. Commercialization of QKD technology could be problematic because the technology relates to both the military and civilian markets. In particular, the military market is large, highly sensitive, bureaucratic, and structured. Thus, each of these markets needs a different approach. Market penetration and size present challenges for these markets. When a market is scattered geographically, the cost of marketing activities and after-sales services are often high; hence, it becomes a challenge for the manufacturer/entrepreneur/innovator of the high technology to have commercial success. Therefore, we argue that market size is important in the commercialization of high technologies because large investments are often involved in developing the technologies; thus, there are must be sufficient markets for such products.

Furthermore, our findings are also in agreement with Szuhaj and McCullough (2009) and Epting and colleagues (2011) in highlighting the importance of building a supply chain. Likewise, the technology validation/certification challenge is in agreement with Pfautsch (2007) because, in a field where a high degree of precision or accuracy is required, such as nanotechnology and QKD technology, technology validation/certification seems to be important. Therefore, technology validation/certification may hinder successful commercialization of QKD technology. For instance, the certification of the high-technology product can be a barrier, especially when the target customers cannot validate the system by themselves or through a third party. In the case study technology, there is no certification yet, and the technology is crucial especially where cybersecurity is a priority, such as in financial institutions, securities agencies, and the military. In addition, our study revealed that the lack of available or adequate infrastructure and after sales-services could hinder the successful commercialization of QKD technology. These two factors have not yet been investigated by the previous scholars.

However, this study has limitations due to its focus on particular high-technology domain and its relatively small sample size. Nonetheless, the case study is highly important to societal security and provides a starting point for further research in other sectors and with other technologies. Studies that investigate the new challenges identified here, especially technology validation/certification and lack of available or adequate infrastructure, would be particularly welcome.

In summary, based on previous studies and our new findings, we conclude that technology validation/certification, lack of available or adequate infrastructure, and after-sales services present challenges to the successful commercialization of high technology, at least in the case of QKD. Similarly, we agreed that market size or market-related issues are the challenges in technology commercialization, as previous studies have shown. In the same view, we confirmed that building a supply chain is among the high-technology commercialization challenges. Therefore, we advise the innovators, inventors, technology entrepreneurs, as well governments to consider these challenges so that their investments in research, development, and innovation are more likely to bring the desired returns.

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

About the Authors

Anas Al Natsheh is a Senior Business Advisor at the Centre for Measurement and Information Systems (CEMIS-Oulu) in Oulu, Finland, and he is a Principal Lecturer in Research, Development, and Innovation (RDI) at Kajaani University of Applied Sciences, also in Finland. He is an expert in empirical researches, research valorization, and technology commercialization. He holds a PhD from the University of Kuopio (now the University of Eastern Finland), where his research focused on the applications of nanotechnology.

Saheed Adebayo Gbadegeshin is a Project Researcher at the University of Oulu in Finland, and he is a Project Staff member at Kajaani University of Applied Sciences, also in Finland. He holds an MSc degree in Entrepreneurship from the University of Jyväskylä in Finland. His research interests include technology-based entrepreneurship, technology commercialization, and family-run businesses.

Antti Rimpiläinen is a Project Researcher at the University of Oulu in Finland and a Project Staff member at Kajaani University of Applied Sciences, also in Finland. He holds an MSc degree in Economics and Business Administration from the University of Oulu in Finland. His research interests include technology-based entrepreneurship, technology commercialization, networking, and international business.

Irna Imamovic-Tokalic is a Project Staff member at the Kajaani University of Applied Sciences in Finland. She holds a BSc degree in Macrofinancial Management from the University of Sarajevo, Bosnia. Her research interests include technology commercialization, digital media and marketing, graphic design, and financial management.

Andrea Zambrano is a Project Researcher at the Kajaani University of Applied Sciences in Finland. She holds a master's degree in Financial and Management Accounting from the University of Oulu in Finland, and in International Economics from the University of Antwerp in Belgium. Her research interests include financial management, research cooperation with Latin-American regions, and economic impact studies with focuses on benefit-cost analyses, financial analyses, and forecasting.

Acknowledgements

We gratefully acknowledge funding received from the European Metrology Research Programme (EMRP) for the Metrology for Industrial Quantum Communication (MIQC) project (Contract IND06). The EMRP is jointly funded by participating countries within EURAMET and the European Union. We also thank our colleagues from the University of Oulu and the Kajaani University of Applied Sciences for their support during the project.

References

Al Natsheh, A., Gbadegeshin, S. A., Rimpiläinen, A., Imamovic-Tokalic, I., & Zambrano, A. 2015. Building a Sustainable Start-Up? Factors to Be Considered During the Technology Commercialization Process. Forthcoming in the *Journal of Advanced Research in Entrepreneurship and New Venture Creation:* http://www.asers.eu/journals/jare_nvc.html

Bulsara, H. P., Gandhi, S., & Porey, P.D. 2010. Commercialization of Technology Innovations and Patents: Issues and Challenges. *Asia-Pacific Tech Monitor,* 27(6): 12–18

Boehlje, M. 2004. Business Challenges in Commercialization of Agricultural Technology. *International Food and Agribusiness Management Review,* 7(1): 91–104.

Booz Allen Hamilton, California HealthCare Foundation, Robert Wood Johnson Foundation, & von Liebig Center for Entrepreneurism and Technology Advancement. 2012. *Accelerating Commercialization of Cost-Saving Health Technologies.*

Chandler, A. D., Jr. 2005. Commercializing High-Technology Industries. *Business History Review,* 79(3): 595–604. http://dx.doi.org/10.1017/S0007680500081460

Chiesa, V., & Frattini, F. 2011. Commercializing Technological Innovation: Learning from Failures in High-Tech Markets. *Product Development & Management Association,* 28(4): 437–454. http://dx.doi.org/10.1111/j.1540-5885.2011.00818.x

Cornford, A. B. 2002. *Innovation and Commercialization in Atlantic Canada: Research Project – Final Report.* Moncton, NB: Atlantic Canada Opportunities Agency (ACOA). http://publications.gc.ca/pub?id=365765&sl=0

Creswell, J. W. 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). London: Sage Publications, Inc.

Epting, T. Gatling, K., & Zimmer, J. 2011. What Are the Most Common Obstacles to the Successful Commercialization of Research? *SML Perspectives,* 2: 9.

Fletcher, A. C., & Bourne, P. E. 2012. Ten Simple Rules to Commercialize Scientific Research. *PLoS Compututational Biology,* 8(9): e1002712. http://dx.doi.org/10.1371/journal.pcbi.1002712

Identifying the Challenges in Commercializing High Technology

Anas Al Natsheh, Saheed A. Gbadegeshin, Antti Rimpiläinen, Irna Imamovic-Tokalic, and Andrea Zambrano

Kalaitzandonakes, N. G. 1997. *Commercialization of Research and Technology*. Washington, D.C.: U.S. Agency for International Development.

Kaarela, M. 2013. *Challenges of Technology Commercialization: Lessons from Finnish-Russian Innovation Alliance on Nanotechnology*. Paper presented at the EuroNanoforum 2013 Workshop on Technology Commercialization, June 18–20, 2013, in Dublin, Ireland. http://www.euronanoforum2013.eu/presentations/presentatins-from-workshops/

Lowe, C. R. 2005. Commercialisation and Spin-Out Activities of the Institute of Biotechnology. *Journal of Commercial Biotechnology,* 11(4): 206–317. http://dx.doi.org/10.1057/palgrave.jcb.3040131

McNeil, R. D., Lowe, J., Mastroianni, T., Croni, J., & Ferk, D. 2007. *Barriers to Nanotechnology Commercialization: Final Report Prepared for U.S. Department of Commerce Technology Administration*. Springfield, IL: The University of Illinois.

Meyers, A. D. 2009. Book Review: Commercialization of Innovative Technologies: Bringing Good Ideas to the Marketplace. *Journal of Commercial Biotechnology,* 15(4): 374–375. http://dx.doi.org/10.1057/jcb.2009.18

Michael, N. T. 1990. Commercializing Technology: What the Best Companies Do. *Planning Review,* 18(6): 20–24. http://dx.doi.org/10.1108/eb054310

Miles, M. B., & Huberman, A. M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.

MIQC. 2014. The Project. *Metrology for Industrial Quantum Communications*. Accessed December 1, 2014: http://projects.npl.co.uk/MIQC/project.html

Nassiri-Koopaei, N., Majdzadeh, R., Kebriaeezadeh, A., Rashidian, A., Yazdi, M. T., Nedjat, S., & Nikfar, S. 2014. Commercialization of Biopharmaceutical Knowledge in Iran: Challenges and Solutions. *DARU Journal of Pharmaceutical Sciences*, 22:29. http://dx.doi.org/10.1186/2008-2231-22-29

Nichols, S. P. 2013. *Module 1: An Introduction to Commercialization of Science and Technology*. Converting Technology to Wealth Workshop. Austin, TX: IC2 Institute, The University of Texas at Austin. Accessed December 1, 2014: http://ut.gtrade.or.kr/inc/download.asp?key=5288

O'Brien, J. N., Blau, J., & Rose, M. 2004. *An Analysis of the Institutional Challenges to Commercialization and Deployment of IGCC Technology in the U.S. Electric Industry: Recommended Policy, Regulatory, Executive and Legislative Initiatives*. New York, NY: Global Change Associates.

Olsen, W. 2004. Triangulation in Social Research: Qualitative and Quantitative Methods Can Really Be Mixed. In Holborn, M. (Ed.), *Developments in Sociology*. Ormskirk, UK: Causeway Press.

Parker, K., & Mainelli, M. 2001. Great Mistakes in Technology Commercialization. *Strategic Change,* 10(7): 383–390. http://dx.doi.org/10.1002/jsc.560

Pellikka, J., Kajanus, M., Heinonen, M., & Eskelinen, T. 2012. *Overcoming Challenges in Commercialization Process of Innovation*. Paper presented at the XXIII ISPIM Conference in Barcelona, Spain. June 17–20, 2012.

Pellikka, J., & Malinen, P. 2011. *Developing Commercialisation of Innovation in High Technology Industries – Regional Perspective*. Paper presented at the 56th International Council for Small Business (ICSB) in Stockholm, Sweden, June 15–18, 2011.

Pfautsch, E. 2007. *Challenges in Commercializing Carbon Nanotube Composites*. Washington, D.C.: Washington Internships for Students of Engineering (WISE).

Rosa, J., & Rose, A. 2007. *Report on Interviews on the Commercialization of Innovation*. Ottawa, CA: Statistics Canada.

Scanlon, K. J., & Lieberman, M. A. 2007. Commercializing Medical Technology. *Cytotechnology*, 53(1-3): 107–112. http://dx.doi.org/10.1007/s10616-007-9056-5

Slater, S. F., & Mohr, J. J. 2006. Successful Development and Commercialization of Technological Innovation: Insights Based on Strategy Type. *The Journal of Product Innovation Management,* 23(1): 26–33. http://dx.doi.org/10.1111/j.1540-5885.2005.00178.x

Speser, P. 2008. *What Every Researcher Needs to Know About Commercialization*. Providence, RI: Foresight Science & Technology Inc.

Szuhaj, M., & McCullough, P. 2009. *Supply Chain Planning and the Commercialization Dead Zone*. Deloitte Consulting LLP. Accessed September 16, 2014: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_lshc_Supply%20Chain%20as%20a%20Blindspot_051209.pdf

Tahvanainen, A., & Nikulainen, T. 2010. *Commercialisation at Finnish Universities: Researchers' Perspectives on the Motives and Challenges of Turning Science into Business. Discussion Paper 1234*. Helsinki: The Research Institute of the Finnish Economy.

Tanev, S., & Frederiksen, M. H. 2014. Generative Innovation Practices, Customer Creativity, and the Adoption of New Technology Products. *Technology Innovation Management Review*, 4(2): 5–10. http://timreview.ca/article/763

Valiauga, P. 2013. *Commercialization of High-tech Radical Innovations: Case Studies of X-ray Imaging Technologies*. Paper presented at the Aalto University School of Science, Finland, May 16, 2013. Accessed December 1, 2014: http://noppa.aalto.fi/noppa/kurssi/tu-22.1500/luennot/TU-22_1500_povilas__commercialisation_of_high-tech_radical_innovations.pdf

Yin, R. K. 1994. *Case Study Research: Design and Methods* (2nd ed.). Thousand Oaks, CA: Sage Publications Inc.

Zawawi, D. 2007. Quantative Versus Qualitative Methods in Social Sciences: Bridging the Gap. *Universiti Putra Malaysia*. Accessed on September 29, 2014: http://psasir.upm.edu.my/809/

Citation: Al Natsheh, A., Gbadegeshin, S. A., Rimpiläinen, A., Imamovic-Tokalic I., & Zambrano, A. 2015. Identifying the Challenges in Commercializing High Technology: A Case Study of Quantum Key Distribution Technology. *Technology Innovation Management Review*, 5(1): 26–36. http://timreview.ca/article/864

Keywords: commercialization, high technology, quantum key distribution, challenges, market size, standards, certification, infrastructure, supply chains, after-sales services

Q&A

Walter Miron

Q. Should the Internet be considered critical infrastructure?

A. In discussing critical infrastructure, Vespignani (2010) put forth the Internet as a "classic example". However, this view is not widely shared. Given its relatively young age, its ongoing amplification, its increasing complexity, and our growing dependence on it, viewing the Internet as a "classic" anything overlooks our need to improve, adapt to, and secure the Internet of the future. Furthermore, even though "information technology" is typically recognized as critical infrastructure, the Internet deserves particular attention as a delivery vehicle for essential services whose disruption holds the potential for societal and financial impacts. Here, I will argue that the Internet should indeed be considered critical infrastructure and that this view will bring benefits in securing it as a delivery vehicle for essential services whose interdependence amplifies the potential impacts of disruptions resulting from failures, natural disasters, and cyber-attacks.

Critical infrastructure is defined as resources that are considered essential to maintaining society, the disruption of which has wide impact on society and the economy (Murray & Grubesic, 2012; Singh et al., 2014; Yusta et al., 2011). Researchers and governments have classified 13 sectors as critical infrastructures, including the general category of "information technology" along with the food supply, banking and finance, telecommunications, defense, emergency services, energy, healthcare, national monuments, shipping, transportation, and water distribution (Singh et al., 2014). In India, however, Internet infrastructure and access is considered one of the critical infrastructure categories (Singh et al., 2014).

Where a failure in one system leads to a failure in another system, these critical infrastructures are said to be interdependent (Vespignani, 2010). Interdependent networks are thought to be fragile compared to an isolated system (Buldyrev et al., 2010; Vespignani, 2010), and the complexity introduced through this interdependency presents design and security challenges (Xiao-Juan & Li-Zhen, 2010). Modern critical infrastructures rely on information and communications technology (ICT) for their control. Rahman and colleagues (2011) define this reliance on ICT as cyber-interdependency and report that data communications account for 85% of failures in cyber-interdependent systems.

Considering the proliferation of high-speed fixed and mobile broadband networks, the delivery of essential services, and the cyber-interdependence that this scenario creates, it can be argued that the Internet has become critical infrastructure. Moreover, considering the Internet as critical infrastructure may help us confront the many challenges relating to the Internet's current design, its regulatory environment, and its cybersecurity assessment practices. In the sections that follow, this argument will be expanded. First, I will consider the amplification of the Internet and its transformation into a critical ICT infrastructure through its use as a delivery vehicle for essential services. Next, I will present definitions of critical infrastructure and cyber-interdependence and compare these definitions to the modern Internet. Finally, I will highlight the need for design practices and frameworks for assessment that may serve to improve the reliability and security of the Internet.

The Internet as a Delivery Vehicle for Essential Services

Essential services such as telephony, broadcast services, online banking and trading, and transportation systems for cross-border trade are increasingly dependent on the reliable and secure operation of the Internet. Simply put, modern communications networks, including the Internet, are critical infrastructures because they deliver essential services (Cetinkaya et al., 2011).

Phahlamohlaka and colleagues (2011) report that, since 2006, the critical national infrastructure in the United States has become increasingly dependent on the Internet. They go on to state that, “The United States economy and government are the most dependent in the world on the Internet.” Consider telephony services: recently, Network World reported that 79% of landline voice customers will switch to other alternatives for voice services such as mobile and Internet phones, and that 47% are already using voice-over-IP products (Hettick, 2014).

Q&A. Should the Internet Be Considered Critical Infrastructure?

Walter Miron

In the financial market, roughly a third of respondents 18 to 44 years of age reported that they used mobile Internet services to conduct banking transactions (U.S. Federal Reserve, 2012). The online payment market transaction volume through Square credit card readers (square.com) has been doubling annually from 2009 to 2013 (Olson, 2014). Delivering financial services over the Internet is another indicator that the Internet is a critical infrastructure.

Transportation and cross-border trade over the Canada–U.S. border contributes 1.8 billion US dollars a day to the economies of both nations with disruptions having major financial impacts (Von Hlatky & Trisko, 2012). Cross-border security has tightened since the September 11th attacks on New York City and the Washington DC metropolitan area, hindering border transit and effectively creating a non-tariff barrier to trade (Von Hlatky & Trisko, 2012). To reduce the impacts to the transportation of goods across this international border, Canada and the United States have launched the Free and Secure Trade (FAST) program that allows low-risk carriers, drivers, and importers expedited border transit (CBSA, 2013). The FAST program allows clearance transactions, applications, and approvals to be conducted online, and implements radio-frequency identification (RFID) technology to minimize delays at border crossings. The use of technology aids in removing non-tariff trade barriers imposed on the transportation of goods and people with heightened security in the post-911 era (Von Hlatky & Trisko, 2012).

The disruption of any of these essential services such as telephony, broadcast services, online banking and trading, and transportation systems for cross-border trade holds the potential for significant impacts to the economy and communications and illustrates that the unintended consequence of the Internet as the great equalizer of innovation leads it to become critical infrastructure by definition due to its cyber-interdependence with the services that it now provides. However, despite this importance, neither regulators nor industry has defined Internet delivery mechanisms in this way nor developed guidelines for improving reliability or security of these assets.

Interdependence of the Internet and Critical Infrastructure

Poljansek and colleagues (2012) consider water, energy, and communications systems as "lifeline utility systems", assigning them special significance due to their interdependence. Disruptions in one part of the network can cause cascading impacts on other parts of the network due to increased traffic of re-routing and other factors (Poljansek et al., 2012; Yusta et al., 2011). Information technology and telecommunications rely on energy, and all other sectors rely on them. Therefore, any disruption to these sectors can lead to adverse impacts to other sectors, (Chapman et al., 2013; Singh et al., 2014). Moreover, critical infrastructures such as public safety and emergency medical services, banking and finance, postal and shipping, healthcare, agriculture and food, transportation, and manufacturing rely heavily on ICT for control and decision making. This cyber-interdependency makes these infrastructures susceptible to ICT failures (Rahman et al., 2011; Singh et al., 2014).

These cyber-interdependencies form a critical situation for Internet delivery of essential services, and infrastructures must be designed, built, and assessed appropriately. However, whereas underlying infrastructure such as electricity or telecommunications are considered to be critical infrastructures, assets deployed in delivering Internet services are not. This discrepancy leads to a situation where, what were once independent essential services delivered to customers on tailored infrastructure elements, may now be delivered together over the Internet without regulatory or industry focus on reliability and security.

Threats to critical infrastructure come in the form of equipment failures, natural disasters, and cyber-attacks. As Vespignani (2010) states, "the most dangerous vulnerability is hiding in the many interdependencies across different infrastructures". When contemplating failures, "near-worst-case scenarios can be as devastating as worst-case scenarios" (Murray & Grubesic 2012).

Independent networks of infrastructure are more fragile than each network in isolation; they fail more abruptly, and at a point of lesser-sustained damage than would an isolated network (Buldyrev et al., 2010). Interdependence of the networks means that "localized damage in one system may lead to a failure in another, triggering cascading and escalating failures" (Vespignani, 2010). This situation further emphasizes the risk to the Internet given its role as a data communications network. One such example of this risk of a cascading event is the Italian power failure of 2003, where power failures impacted communications and the Internet, which in turn further impacted power stations (Buldyrev et al., 2010). Human factors are another key source of failures. Of all critical infrastructure disruptions, 85% are attributable to the failure of data commu-

Q&A. Should the Internet Be Considered Critical Infrastructure?

Walter Miron

nications networks (Rahman et al., 2011), and human-related failures account for 50% of Internet disruptions (Cetinkaya et al., 2011).

Infrastructures are dependent on and impacted by the environments in which they operate, making them susceptible to natural disasters (Poljansek et al., 2012). Water, transportation, fuel, and power are coupled together (Buldyrev et al., 2010), and failures in any of these domains will have cascading affects on other domains. Hurricanes Katarina and Andrew in the United States and the Fukijama Earthquake in Japan are examples of the impact of the environment on critical infrastructures.

However, not all human failures originate from errors. Cyber-attacks are on the rise, and our increasing connectedness, data, and flows provide more opportunities for exploitations by actors with malicious intent (Dupont, 2013). Due to their interdependency, energy, information technology, and telecommunications are the main cascade-initiating sectors and therefore are primary targets for malicious attacks (Singh et al., 2014). Recent military actions in Georgia and Estonia were coordinated with attacks on Internet resources and were aimed at impacting interdependent critical infrastructure in the financial, industrial, and control infrastructures (Phahlamohlaka et al., 2011).

The increase in both volume and sophistication of cyber-attacks as well as the increase in natural disasters supports a call for the development of guidelines for building and assessing reliability and security readiness of Internet assets. Next, I will discuss steps that can be taken to address the risk of failure of essential services due to disruptions of the Internet.

Recognizing the Internet as Critical Infrastructure

The interdependency between critical infrastructure elements is a key factor in effectively securing them (Xiao-Juan, & Li-Zhen, 2010). Thus, our growing dependency on ICT corresponds with the increasing importance of protection designs for critical infrastructures (Merabti et al., 2011). Therefore designing for resiliency is important because networks cannot be built for true 100% availability (Cetinkaya et al., 2011). These designs for critical infrastructure protection should include diversification, separation, avoidance, and hardening strategies (Murray & Grubesic, 2012). However, significant investments of human and financial resources are required to fortify critical infrastructure, including the Internet (Cetinkaya et al., 2011; Murray & Grubesic, 2012).

Regulators and academics have expressed interest in protecting critical infrastructure (Poljansek et al., 2012); however, this interest has not led to frameworks prescribing action to treat the Internet as critical infrastructure. Current initiatives at federal, sub-federal, and local levels lack methodological frameworks for evaluating infrastructure protection (Murray & Grubesic, 2012), and with cyber-capabilities outpacing methodologies and legal frameworks for operational control (Phahlamohlaka et al., 2011), priority must be placed on protecting these critical infrastructures by state and federal governments (Singh et al., 2014). Given that Internet access and assets are primarily owned and operated privately, cooperation between the owners and government agencies is required, along with regulatory oversight (Murray & Grubesic, 2012).

Conclusion

To successfully rise to the challenges of building and securing reliable cyber-interdependent networks for the delivery of services such as Internet telephony, online banking, trading, and payment processing , I argue that we must consider the Internet as critical infrastructure. To complement this view, I recommend the development and adoption of a framework for designing in security and reliability and assessing the readiness of interdependent networks of critical infrastructure.

Reliability and security of networks on the scale of the Internet require significant investments of time, resources, and funding. Owing to the private ownership of most Internet delivery resources, and the competition in the Internet access market and the services delivered over it, public and private cooperation is required in defining and implementing a framework for the construction, security, and assessment of these critical infrastructures and key resources. In addition to the regulatory oversight needed to ensure reliable and secure operation of these key resources, business models are needed that recognizes the value of reliability and security in the delivery of essential services over the Internet.

Considering the maturation of the Internet into a delivery vehicle for essential communications and financial, trading, and broadcast services, the complexities of designing reliable and secure interdependent networks of critical infrastructure, and the increase in the volume and sophistication of cyber-attacks as well as natural

Q&A. Should the Internet Be Considered Critical Infrastructure?

Walter Miron

disasters, the Internet must become broadly recognized as critical infrastructure. To do so would represent an opportunity for the industry, researchers, and regulators to cooperate to ensure the reliable and secure operation of the future Internet.

About the Author

Walter Miron is a Director of Technology Strategy at TELUS Communications, where he is responsible for the evolution of their packet and optical networks. He has over 20 years of experience in enterprise and service provider networking conducting technology selection and service development projects. Walter is a member of the research program committee of the SAVI project, the Heavy Reading Global Ethernet Executive Council, and the ATOPs SDN/nFV Working Group. He is also the Chair of the Venus Cybersecurity Corporation and is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada.

References

Buldyrev, S., Shlomo, H., Roni, P., Gerald, P., & Eugene, S. 2010. Catastrophic Cascade of Failures in Interdependent Networks. *Nature,* 464(7291): 1025–1028. http://dx.doi.org/10.1038/nature08932

CBSA. 2013. Free and Secure Trade (FAST). *Canadian Border Services Agency.* Accessed January 10, 2015: http://www.cbsa-asfc.gc.ca/prog/fast-expres/menu-eng.html

Çetinkaya, E. K., Broyles, D., Dandekar, A., Srinivasan, S., & Sterbenz, J. P. 2013. Modelling Communication Network Challenges for Future Internet Resilience, Survivability, and Disruption Tolerance: A Simulation-Based Approach. *Telecommunication Systems,* 52(2): 751–766. http://dx.doi.org/10.1007/s11235-011-9575-4

Chapman, L., Azevedo, J. A., & Prieto-Lopez, T. 2013. Urban Heat & Critical Infrastructure Networks: A Viewpoint. *Urban Climate,* 3: 7–12. http://dx.doi.org/10.1016/j.uclim.2013.04.001

Dupont, B. 2013. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review,* 3(7): 6–11. http://timreview.ca/article/700

Hettick, L. 2014. Surveys Point to Increased Adoption of VoIP and Wireless Substitution. *Network World.* Accessed January 10, 2015: http://www.networkworld.com/article/2455174/

Merabti, M., Kennedy, M., & Hurst, W. 2011. Critical Infrastructure Protection: A 21st Century Challenge. In *Proceedings of the International Conference on Communications and Information Technology (ICCIT 2011):* 1–6. Washington, DC: IEEE. http://dx.doi.org/10.1109/ICCITECHNOL.2011.5762681

Murray, A. T., & Grubesic, T. H. 2012. Critical Infrastructure Protection: The Vulnerability Conundrum. *Telematics and Informatics,* 29(1): 56–65. http://dx.doi.org/10.1016/j.tele.2011.05.001

Olson, P. 2014. Square Strikes Nationwide Payment Deal With Whole Foods. *Forbes.* Accessed January 10, 2015: http://www.forbes.com/sites/parmyolson/2014/02/11/square-strikes-nationwide-payment-deal-with-whole-foods/

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. 2011. Cyber Security Awareness Toolkit for National Security: An Approach to South Africa's Cyber Security Policy Implementation. In *Proceedings of the first IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW 2011):* 1–14. Laxenburg, Austria: International Federation for Information Processing. http://hdl.handle.net/10204/5162

Poljanšek, K., Bono, F., & Gutiérrez, E. 2012. Seismic Risk Assessment of Interdependent Critical Infrastructure Systems: The Case of European Gas and Electricity Networks. *Earthquake Engineering & Structural Dynamics,* 41(1): 61–79. http://dx.doi.org/10.1002/eqe.1118

Rahman, H. A., Martí, J. R., & Srivastava, K. D. 2011. A Hybrid Systems Model to Simulate Cyber Interdependencies between Critical Infrastructures. *International Journal of Critical Infrastructures,* 7(4): 265–288. http://dx.doi.org/10.1504/IJCIS.2011.045056

Singh, A. N., Gupta, M. P., & Ojha, A. 2014. Identifying Critical Infrastructure Sectors and their Dependencies: An Indian Scenario. *International Journal of Critical Infrastructure Protection,* 7(2): 71–85. http://dx.doi.org/10.1016/j.ijcip.2014.04.003

U.S. Federal Reserve. 2012. FRB: Current Use of Mobile Banking and Payments. *Board of Governors of the Federal Reserve System.* Accessed January 10, 2015: http://www.federalreserve.gov/econresdata/mobile-devices/2012-current-use-mobile-banking-payments.htm

Vespignani, A. 2010. Complex Networks: The Fragility of Interdependency. *Nature,* 464(7291): 984–985. http://dx.doi.org/10.1038/464984a

Von Hlatky, S., & Trisko, J. N. 2012. Sharing the Burden of the Border: Layered Security Co-operation and the Canada–US Frontier. *Canadian Journal of Political Science,* 45(1): 63–88. http://dx.doi.org/10.1017/S0008423911000928

Xiao-Juan, L., & Li-Zhen, H. 2010. Vulnerability and Interdependency of Critical Infrastructure: A Review. In *Proceedings of the Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA 2010):* 1–5. Washington, DC: IEEE. http://dx.doi.org/10.1109/INFRA.2010.5679237

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. 2011. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art. *Energy Policy,* 39(10): 6100–6119. http://dx.doi.org/10.1016/j.enpol.2011.07.010

Citation: Miron, W. 2015. Q&A. Should the Internet Be Considered Critical Infrastructure? *Technology Innovation Management Review,* 5(1): 37–40. http://timreview.ca/article/865

Keywords: cybersecurity, Internet, critical infrastructure, cyber-attacks, vulnerabilities, information technology, communication networks

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