Conference Proceedings of

18th Australian Cyber Warfare Conference 2019 (CWAR 2019), October 7-8, 2019, Melbourne, Victoria, Australia.

Edited by:
Matthew Warren
ISBN. 978-0-6484570-2-2.

Proceedings of

CWAR 2019

Edited by
Matthew Warren
ISBN 978-0-6484570-2-2.

Organised By:

Deakin University Centre for Cyber Security Research and Innovation

Sponsor:

Australian Information Security Association.

Published by the Deakin University Centre for Cyber Security Research and Innovation, Deakin University, Geelong, Victoria, Australia.

Welcome

The 18th Australian Cyber Warfare (formally Information Warfare) conferences builds upon a number of national conferences run across Australia namely in Perth, Melbourne, Geelong and Adelaide.

This conference looks at the continued development of Cyber Security within Australia, taking into the new emerging technologies and approaches.

Papers were selected for their relevance in relation to Cyber Security and the conference theme. The aim of this conference is to further the work already achieved within Australia and bring together researchers in the field to discuss the latest issues and their implications upon Australia. All full papers were reviewed by two members of the program committee. This year papers came from Australia (ACT, VIC, WA), Lithuania, Saudi Arabia and USA.

We commend the author for their hard work and sharing their results, and the reviewers of the conference for producing an excellent program.

CWAR 2019 Organising Committee

Conference Chair
Matthew Warren, Centre for Cyber Security Research and Innovation, Deakin University, Australia

Program Committee
Andy Jones, University of Hertfordshire, United Kingdom.
Atif Ahmad, University of Melbourne, Australia.
Bill Hutchinson, Edith Cowan University, Australia.
Darius Štitilis, Mykolas Romeris University, Lithuania.
Debi Ashenden ,Deakin Univeristy, Australia.
Graeme Pye, Deakin University, Australia.
Jeff Malone, Department of Defence, Australia
Jill Slay, La Trobe University, Australia.
Johan Van Niekerk, Nelson Mandela University, South Africa.
Mathews Nkhoma, RMIT Vietnam, Vietnam.
Martti Lehto ,University of Jyväskylä, Finland.
Mike Johnstone, Edith Cowan University, Australia.
Oliver Burmeister, Charles Sturt University, Australia.
Sean Maynard, University of Melbourne, Australia.
Shona Leitch, RMIT, Australia.
Steven Furnell, University of Plymouth, United Kingdom.
Paul Haskell-Dowland, Edith Cowan University, Australia.
Raymond Choo, University of Texas at San Antonio, United States of America.
Regina Valutyte, Mykolas Romeris University, Lithuania.

Contents

What is Cyber Terrorism: Discussion of Definition and Taxonomy

Jordan J. Plotnek, Jill Slay

***Abstract*— This paper reviews the use of the term 'cyber terrorism' and proposes a new universally-applicable taxonomy and definition. The proposed new definition is derived from detailed analyses of existing definitions in the publicly available literature, which includes all of the key commonalities identified in accordance with the newly proposed taxonomy and allows for more specific subsets of cyber terrorism to be defined in future research.**

***Index Terms*—Cybersecurity, cyber terrorism, definition, taxonomy, terrorism.**

I. Introduction

Cyber Terrorism is a relatively young field and hence there is a notable shortage of reputable literature to inform policy, guide public discussion, and drive decision-making. One fundamental issue that remains unsolved and is delaying all other developments in this area is the question of definition – what is cyber terrorism? A number of definitions have been proposed since the mid-eighties, however none of these definitions have proved sufficient for universal adoption. The goal of this paper is to analyse the major definitional contributions over time in order to propose a unified definition, grounded in existing literature and current usage.

II. Taxonomy and Definition

In order to make sense of the various aspects of cyberterrorism that have emerged in this growing field, [1] made a first attempt to define a cyber terrorism taxonomy using five key components: Target, Motive, Means, Effect, and Intention. The taxonomy proposed by [1] captures most of the attributes found throughout the existing cyber terrorism definitions, however after applying it to the analysis of previously proposed definitions it was found to be lacking one key component. In addition to the already specified components of the taxonomy at [1], existing cyber terrorism definitions were found to also differ with respect to who constitutes a cyber terrorist (e.g. non-state actors, terrorist groups, nation states, undefined, etc.). Therefore a revised taxonomy is proposed in Figure 1, which includes the aforementioned five components from [1] but with an additional component, Actor.

There is no universally accepted definition of cyber terrorism. The term cyber terrorism was first coined in the mid- eighties by Barry C. Collin, a senior person research fellow of the Institute for Security and Intelligence in California [2]. Collin had, at that time, defined cyber terrorism simply as "the convergence of cybernetics and terrorism". Due to this definition's over-simplicity and resulting lack of specificity, a myriad of other attempts at defining cyber terrorism have since emerged in the literature. The confusion surrounding cyber terrorism is even moreso apparent in public discourse and media usage; as examined in depth in [3], where the authors analysed 535 articles across 31 media outlets that used the term cyber terrorism between 2008 and 2013.

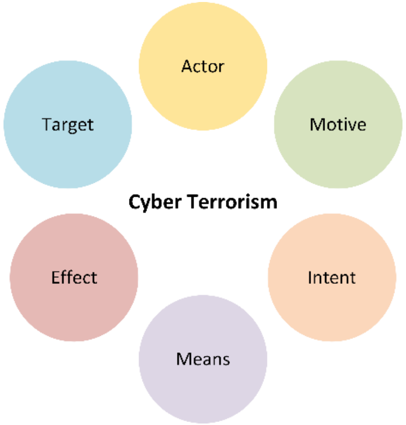


Figure 1: New cyber terrorism taxonomy, revised from [1]

A large proportion of the definitions available in the literature have arisen out of the need for jurisdiction-specific legal terminology to aid with deterrence and prosecution of would-be cyber-terrorists [4], and therefore are not broad enough to apply on a global scale. Another driving factor that complicates the ability for a unified definition includes the ongoing evolution and widely acknowledged inconsistency of the use of the parent term, "terrorism". Additionally, definitions for cyber terrorism are even further complicated by the fact that they must be specific enough to be understood distinctly from other types of cyberattack, such as cyber warfare and hacktivism [5].

III. Definition Analysis

Given the ongoing debate surrounding the scope and nature of cyber terrorism, this term can become confusing to use as a benchmark for which to legislate and protect against. As such, it is beneficial to define "cyber terrorism" in a broad manner that includes all the key features witnessed in existing literature, and then from this define specific subsets as distinct aspects of the broader definition that are purpose-specific (e.g. "cyber-physical terrorism" for critical infrastructure protection).

In order to do this effectively, the key features of cyber terrorism, as defined in the literature, must first be identified; noting that more recent literature emphasises aspects relating to threat intent [6], [7]. Figure 2 displays the common requisite features of cyber terrorism as found in the literature. Additional guidance can also be sought from [8], where the authors had surveyed 115 researchers and policymakers on what they deem to be important elements of cyberterrorism.

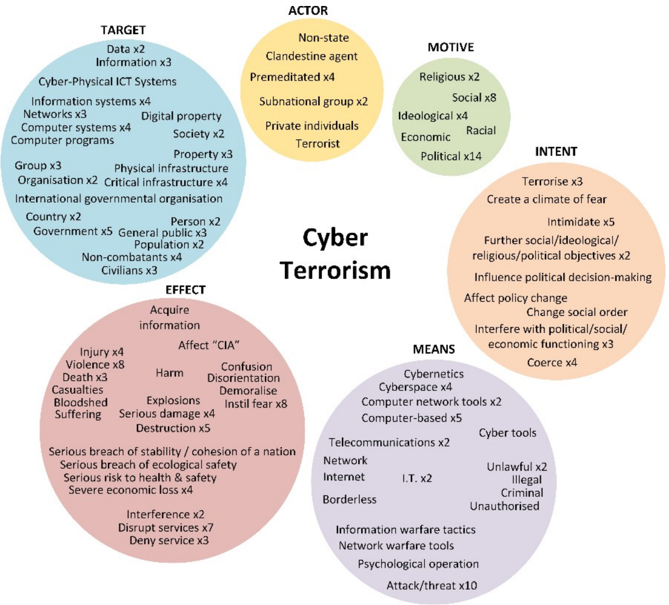


Figure 2: Features inherent to cyber terrorism, as defined in current literature, grouped according to the taxonomy at Figure 1. An 'x' is used to denote the number of occurrences where the term appeared more than once.

The first of the six cyber terrorism features at Figure 1, 'Actor', describes the requisite traits of the so-called cyber terrorist. Within this category there are six unique attributes that emerge in the literature; non-state, clandestine agent, premeditation, subnational group, private individuals, and terrorist, as shown in Figure 2. These can be grouped into four distinct attributes that describe a cyber terrorist actor, which in order of frequency are: non-state, premeditated, terrorist, and clandestine. Of these four categories, non-state and premeditated were far more prescribed than being a terrorist (by the traditional definition) or clandestine. It is also worth noting that the 'clandestine' label, although seemingly broad enough to include state actors, actually appeared within a definition limited to subnational groups as a concurrent prerequisite for cyber terrorists [9]. As such, amongst the authors that included a description of the actor within their proposed cyber terrorism definitions, there appears to be general agreement that a cyber terrorist is a non-state actor that plans out their attacks as opposed to acting out of spontaneity.

The second feature in the cyber terrorism taxonomy at Figure 1 is 'Motive', which is concerned with the motivating factors behind a cyber terrorism plot. Figure 2 highlights six different motives identified within the surveyed literature; religious, social, ideological, racial, economic, and political. These six descriptions can be simplified into three common categories, which in order of frequency are: ideological (including religious, political, ideological), social (including racial and social), and economic. There was found to be a clear preference in the literature towards defining ideological and social motives as being primary drivers behind cyber terrorism. This is also consistent with the findings at [8].

'Intent' is the third component of the updated cyber terrorism taxonomy at Figure 1 and describes a cyber terrorist's intended goals. Figure 2 shows that nine different phrases emerged from the literature regarding the current academic understanding of a cyber terrorist's intent. These nine phrases have been condensed into five general objectives; coerce, induce fear, interfere, effect change, and further objectives. There were 21 overall prescriptions of intent for an act or threat thereof to be classified as cyber terrorism, with a strong leaning towards coercion being the primary intention (67% of prescribed intent characteristics relate to coercion and inducing fear).

The final three components of the cyber terrorism taxonomy were found to have the most definitional diversity. Starting with 'Means', 17 differing descriptions were identified, with nine overall concepts emerging; attack or threat of attack, computer, cyberspace, network, illegal, cyberwarfare, unauthorised, borderless, psychological operations. It is interesting to note that an actual attack or a threat of attack was only required ten times in the surveyed definitions, with a number of these instances occurring within the same statement (e.g. [10]). Also worth noting is that cyberspace, computer, and network were only mentioned 19 times, also with some of these occurring within the same definition. The final two categories, cyberwarfare and psychological operations, are quite peculiar as they are generally ascribed to state-sponsored military operations. The term 'cyberwarfare', in particular, is an entirely separate category of cyber operations and cyberattack that has its own ongoing definitional battles. In fact, a significant proportion of the surveyed literature went to great efforts to distinguish cyber terrorism from other types of cyber operations such as cyberwarfare (see [5], for example). Psychological operations is less contradictory as it can, and most likely would, occur alongside a cyber terrorism plot; however much like with cyberwarfare, the term carries its own weight and distinct definitions and debates, and so is problematic for inclusion in the definition of cyber terrorism.

'Effect' was attributed 23 different statements in Figure 2, each with varying levels specificity and severity. These have been grouped under seven categories; violence, service disruption, psychosocial impact, physical damage, economic damage, data breach, and ecological damage. By far the four most agreed-on effects of cyber terrorism are violence, service disruption, physical damage, and psychosocial impact; each of which emerged at significantly higher rates than the three least common. Violence is a standout attribute, with 19 separate definitions using this as a requisite effect of cyber terrorism. Of the three least common effects cited in the surveyed definitions, ecological and economic damage appeared as potential, but not necessary, effects of cyberterrorism, whilst data breach (i.e. unauthorised access to information) was used in a way that is inconsistent with the rest of the literature and conflicts with the required intentions described earlier. The key theme amongst the defined effects seems to be an impact or effect that occurs outside of cyberspace, whether that be psychological, social, political, physical, economic, or ecological.

The final attribute in the cyber terrorism taxonomy is 'Target'. Figure 2 shows the 22 different descriptions of what constitutes a cyber terrorist's target according to the currently available literature. From these descriptions seven categories were established (civilians, ICT, physical infrastructure, government establishments, data, non-government establishments, and software), three of which are digital in nature, one which is physical, and three that are human-oriented. The number one most commonly cited target throughout the surveyed definitions was 'civilians' (i.e. general public, population, non-combatants, civilians, persons, and society), which together appeared 16 times. The three technologically-oriented targets (data, software, and

ICT) don't provide much value in the way of understanding exactly what is being targeted as they could describe almost any technology these days; not to mention that they also don't fall firmly within the restriction of generating effects outside of cyberspace as concluded earlier. Finally, both government and non-government establishments were defined as targets 13 times in total. Each of these targets have obvious links with the intent of the cyber terrorist; for example, if fear is the desired outcome then a civilian target might make sense, however if the intent is disruption then perhaps a technological or organisational target would be selected. In combination with the other factors, each of these targets would result in slightly differing campaigns, whilst still remaining identifiable as cyber terrorism. From this analysis it can be seen that the scope of what might constitute the target of cyber terrorism is largely variable, entirely dependent on the cyber terrorist's intent. This not only confirms the need for more specific sub-definitions of cyber terrorism (such as cyber-physical terrorism), but also demonstrates the need for generality in the attribution of a target to the broader definition of cyber terrorism itself.

IV. New Definition: discussion and conclusion

All up, Figure 3 demonstrates that 'Effect' and 'Target' are by far the most prescribed elements throughout the literature, having been defined 61 and 56 times respectively. By contrast, the 'Actor' element carries far less importance in the surveyed definitions, having only been described as a requisite feature ten times throughout the literature, with all other definitions leaving the type of perpetrator open to any actor (e.g. state actors).

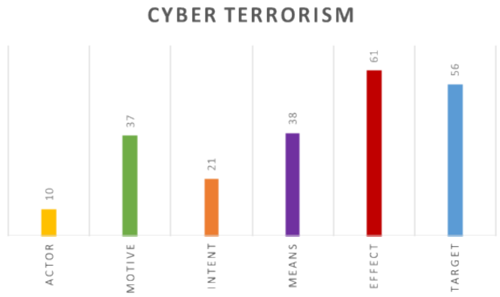


Figure 3: Summary of attributes ascribed to each element of the cyber terrorism taxonomy at Figure 1 throughout existing cyber terrorism definitions

This result could be due to a few different reasons. The first and perhaps most obvious one is that a single actor can cause multiple different effects on numerous targets, and hence more target/effect attributes might be able to be described than the qualities inherent to a cyber terrorist actor. Another reason for this disparity could be that certain aspects of the taxonomy, such as intent, might be better understood (stemming from pre-existing research into traditional terrorism, for example) and hence can be described more efficiently than other aspects. Finally, such a disparity could indeed indicate the comparative definitional importance between each element of the taxonomy (e.g. target and effect may be more important elements of cyber terrorism than actor or intent). Acknowledging that the answer is likely a combination of these speculations, it provides the most utility to treat each element of the taxonomy in its own right and avoid diminishing attention to any particular aspect. This is reinforced by the observation that 'Means' is only seen to make up 17% of the weight in Figure 3 despite the fact that this element is inherent to the term *cyber* terrorism.

In light of the findings detailed throughout this section it is now possible to construct a new universally applicable definition of cyber terrorism that acknowledges the major contributions to the subject up until now. In order to do this the important attributes ascribed to each element of the taxonomy must first be summarised, the results of which are listed below:

- Actor: premeditated, non-state
- Motive: ideological, social
- Intent: induce fear, coerce
- Means: attack or threat of attack, originates in cyberspace
- Effect: a consequence that occurs outside of cyberspace (e.g. psychological, social, political, physical, economic, ecological)
- Target: civilian, government, non-government.

Having identified the critical attributes arising from existing definitions in the literature, aligned to the newly proposed cyber terrorism taxonomy, a new definition may now be proposed as such:

"Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace to cause real-world consequences in order to induce fear or coerce civilian, government, or non- government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychosocial, political, economic, ecological, or otherwise that occur outside of cyberspace."

From this broad universally-applicable definition, further research can work to define specific subsets for particular usage, such as 'cyber-physical terrorism' for critical infrastructure protection.

References

[1] A. Al Mazari, A. H. Anjariny, S. A. Habib, and E. Nyakwende, "Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies," in *Cyber Security and Threats Concepts Methodologies Tools and Applications*, 2018, p. chapter 32.

[2] B. Akhgar, A. Staniforth, and F. Bosco, Eds., *Cyber Crime and Cyber Terrorism Invesitgators Handbook*. Elsevier Syngress, 2014.

[3] L. Jarvis, S. Macdonald, and A. Whiting, "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat," *European Journal of International Security*, vol. 2, no. 1, pp. 64–87, Sep. 2016.

[4] K. Hardy and G. Williams, "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism," in *Cyberterror- ism Understanding Assessment and Response*. New York: Springer Science+Business Media, May 2014, pp. pp. 1–24.

[5] M. Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis*, vol. 59, no. 1, pp. 111–128, 2015.

[6] Z. Yunos, N. Mohd, A. Ariffin, and R. Ahmad, "Understanding Cyber Terrorism From Motivational Perspectives: A Qualitative Data Analysis," in European Conference on Cyber Warfare and Security, Dublin, Ireland, Jun. 2017.

[7] S. Macdonald, L. Jarvis, and T. Chen, "Cyberterrorism Project Research Report," in A Multidisciplinary Conference on Cyberterrorism, Swansea University, UK, 2013.

[8] L. Jarvis and S. Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers," *Taylor and Francis Terrorism and Political Violence*, vol. 27, no. 4, pp. 657–678, May 2014.

[9] H. Stambaugh, D. S. Beaupre, D. J. Icove, R. Baker, W. Cassaday, and W. P. Williams, "Electronic Crime Needs Assessment for State and Local Law Enforcement," National Institute of Justice, Washington DC, Tech. Rep., Mar. 2001.

[10] C. Bryan Foltz, “Cyberterrorism, computer crime, and reality,” *Informa- tion Management & Computer Security*, vol. Vol. 12, no. No. 2, pp. pp. 154–166, Apr. 2004.

[11] R. M. Lee, M. J. Asssante, and T. Conway, “Analysis of the cyber attack on the Ukrainian power grid,” Mar. 2016.

[12] B. Sobczak, “’Cyber event’ disrupted U.S. grid networks - DOE,” https://www.eenews.net/stories/1060242741, Apr. 2019.

[13] N. Beecroft and et al., “Business Blackout - The insurance implications of a cyber attack on the US power grid,” University of Cambridge, Centre for Risk Studies, Tech. Rep., May 2015.

[14] J. E. Moore, The Economic Costs and Consequences of Terrorism. Edward Elgar Publishing, Jan. 2008.

[15] T. S. Popik, “Testimony of the Foundation for Resilient Societies,” in Reliability Technical Conference. Federal Energy Regulatory Commission, Jun. 2017.

[16] P. Wang, “Death by Hacking: The Emerging Threat of Kinetic Cyber,” in Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications. Singapore: Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Jul. 2019, p. 17.

[17] C. Glenn, D. Sterbentz, and A. Wright, “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector,” Tech. Rep. INL/EXT–16-40692, 1337873, Dec. 2016.

[18] K. Lab, “Threat landscape for industrial automation systems,” ICS CERT, Tech. Rep., Mar. 2019.

[19] N. Kshetri and J. Voas, “Hacking Power Grids: A Current Problem,” Computer, vol. 50, no. 12, pp. 91–95, Dec. 2017.

[20] AustralianGovernment, “2017 Foreign Policy White Paper,” 2017.

[21] D. Kellner, Media Spectacle and the Crisis of Democracy: Terrorism, War, and Election Battles. Routledge, Dec. 2015.

[22] B. Nacos, Mass-Mediated Terrorism: Mainstream and Digital Media in Terrorism and Counterterrorism. Rowman & Littlefield, Feb. 2016.

[23] M. M. Pollitt, “Cyberterrorism—Fact or Fancy?’,” Elsevier Computer Fraud & Security, no. issue 2, pp. pp. 8–10, Feb. 1998.

[24] D. Denning, “Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism,” U.S. House of Representatives, May 2000.

[25] J. A. Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,” Center for Strategic and International Studies, Dec. 2002.

[26] R. Nagpal, “Cyber Terrorism in the Context of Globalization,” in Second World Congress on Informatics and Law, Madrid, Spain, Sep. 2002, pp. 1– 23.

[27] G. Weimann, “Cyberterrorism: The Sum of all Fears?” Taylor & Francis, Studies in Conflict & Terrorism, vol. Vol. 28, no. Issue 2, p. 130, Aug. 2004.

[28] P. Czerpak, “The European Dimension of the Flight against Cyberterrorism – A Theoretical Approach,” in Europe and Complex Security Issues, 2005, pp. 309–318.

[29] DCSINT, Critical Infrastructure Threats and Terrorism: Handbook. Kansas: Deputy Chief of Staff for Intelligence, 2006, vol. 1.

[30] D. Denning, “A View of Cyberterrorism Five Years Later,” in Internet Security: Hacking, Counterhacking, and Society. London: Jones and Bartlett, 2007, pp. 123–140.

[31] B. Mantel, “Terrorism and the Internet: Should Web sites that promote terrorism be shut down?” CQ Global Researcher, vol. 3, no. 11, Nov. 2009.

[32] K. Mshvidobadze, “State-sponsored Cyber Terrorism: Georgia’s Experience,” Tbilisi, Georgia, Sep. 2011.

[33] J. Hua and S. Bapna, “How Can We Deter Cyberterrorism?” Taylor & Francis, Information Security Journal: A Global Perspective, vol. 21, no. 2, pp. 102– 114, Apr. 2012.

[34] O. Bosch, “Critical Information Infrastructure and Cyber-Terrorism,” in Law, Policy, and Technology - Cyberterrorism, Information Warfare, and Internet Immobilization. Hersey, PA: Information Science Reference, 2012, pp. 31– 40.

[35] K. O. Osman, W. R. S. Osman, Y. Al-Khasawneh, and S. Duhaim, “Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea,” International Journal of Computer Science and Mobile Computing, vol. Vol. 3, no. 5, pp. 1082–1090, 2014.

[36] Z. Yunos, R. Ahmad, and N. A. Mohd Sabri, “A Qualitative Analysis for Evaluating a Cyber Terrorism Framework in Malaysia,” Information Security Journal: A Global Perspective, vol. 24, no. 1-3, Apr. 2015.

Unsupervised Anomaly-based Intrusion Detection for SCADA Systems

Abdullah M. Alsaedi[1,a], Abdulmohsen Almalawi[2,b], Zahir Tari[1]
[1]RMIT University, School of Science, Melbourne, Australia
[2]King Abdulaziz University, School of Computer Science & Information Technology, Jeddah, Saudi Arabia
[a]abdullah.mohammed.alsaedi@rmit.edu.au; [b]balmalowy@kau.edu.sa

Abstract. Supervisory Control And Data Acquisition (SCADA) systems have become a core part of controlling and monitoring critical infrastructures such as energy grids, power plants, and water distribution systems. In recent years, such systems have become highly vulnerable to cyber-attacks. Hence, to counter such attacks, the design of efficient, unsupervised anomaly detection solutions has become an important topic of interest relating to the development of SCADA-specific Intrusion Detection Systems (IDSs). This paper discusses a proposed unsupervised anomaly-based IDS solution for SCADA that is data-driven and does not require prior knowledge of the physical behaviour of the systems. Moreover, the proposed solution is based on two novel ideas: an automatic identification of consistent and inconsistent states of SCADA data for any given system, and an automatic extraction of proximity detection rules from identified states. This is based on a data-driven clustering technique of process parameters, which automatically identifies the normal and critical states of a given system. The proposed solution works in an unsupervised mode where labeled training data is not required, and it does not require the involvement of an expert to extract detection rules. This will help to reduce time-expensive processing and eliminate human errors.

Keywords**:** Supervisory Control and Data Acquisition, SCADA, Intrusion Detection System, anomaly detection.

Introduction

Supervisory Control and Data Acquisition (SCADA) systems have been introduced to control and monitor critical infrastructures and industrial processes such as power generation and water distribution (Boyer 2009**)**. However, any disruption to SCADA systems can result in catastrophic consequences such as financial losses and serious impact on public safety and the environment. The attack on a sewage treatment system in Maroochy Shire, Queensland, is an obvious example of the seriousness of cyber-attacks on critical infrastructures (Slay & Miller 2007). Moreover, Stuxnet (Falliere et al. 2011), Duqu (Bencsáth et al., 2012) and Flame (Munro, 2012) are some cyber-attacks that were initiated from inside the automation system itself. Therefore, it is vital that these systems be secured and protected. The potential threats to SCADA systems and the need to reduce risk and mitigate vulnerabilities has recently emerged as an interesting research topic in the security area. Several security measures such as firewalls, encryption and intrusion detection have been extensively used in traditional IT. However, these measures cannot be applied directly to SCADA systems without considering their different nature and characteristics. Moreover, none of these security measures can completely protect a system from potential threats. However, a full complement of these measures can create a robust security system.

An Intrusion Detection System (IDS) is one of the security solutions that has demonstrated promising results in detecting malicious activities in traditional IT systems, and therefore it has been adapted in SCADA systems (Fovino et al. 2010). The differences between the nature and characteristics of traditional IT and SCADA systems (e.g. real-time processing, high availability of data and processes) have motivated security researchers to develop SCADA-specific IDSs. IDSs are categorised according to two approaches: *signature-based detection* and *anomaly detection*. The *former* can detect only known attacks because it monitors the system against specific patterns of attacks (Yang et al. 2013). On the other hand, the *latter* attempts to learn the normal behaviour of the systems, and any deviation from this behaviour is assumed to be a malicious activity (Linda et al. 2009). Both approaches have advantages and disadvantages. The former achieves good accuracy but fails to detect attacks that are new or the patterns of which are not learned. Although the latter can detect novel attacks, the overall detection accuracy of this approach is low. In addition, there are two types of anomaly detection techniques: *supervised*, *semi-supervised* and *unsupervised* modes. In the supervised mode, training data are labelled, while in the semi-supervised it is assumed that the training data set represents only one behaviour, either normal or abnormal. In the unsupervised mode, data are not labelled (Bhuyan et al. 2014).

The monitoring of the behaviour of SCADA systems through the evolution of SCADA data has attracted the attention of researchers (Jin et al., 2006; Rrushi 2009; Zaher et al. 2009; Gao et al. 2010; Marton et al. 2013; Alcaraz & Lopez 2014). (Jin et al., 2006) extended the set of invariant models with a value range model to detect any inconsistent value for a particular data point. Similarly, (Alcaraz & Lopez 2014) monitor each data point (sensory node) individually using predefined thresholds (e.g., min, max), and any reading that is not inside a prescribed threshold is considered as an anomaly. These approaches are effective for monitoring one single data point. However, although the value of an individual data point may not be abnormal, in combination with other data points, it may produce an abnormal observation, which very rarely occurs. To address the aforementioned issues, some studies have been proposed to design SCADA anomaly detection solutions that learn the behaviour of SCADA systems through the evolution of SCADA data instead of using predefined thresholds (Rrushi 2009; Zaher et al. 2009; Carcano et al., 2011; Gao et al. 2010; Marton et al. 2013). Such studies however can operate in only two learning modes: *supervised* and *semi-supervised*. There are several issues pertaining to these modes. The system has to operate for a long time under normal conditions in order to obtain purely normal data that comprehensively represent normal behaviours. However, there is no guarantee that any anomalous activity will occur during the data collection period. Nonetheless, it is difficult to obtain a training data set that covers all possible anomalous behaviours that could occur in the future. Thus, the unsupervised mode may be an appropriate solution to address the aforementioned issues, where the anomaly detection models can be learned from unlabelled data without prior knowledge about normal and abnormal behaviours.

This paper discusses an unsupervised SCADA-specific IDS solution, which consists of two novel techniques. The first one is used to identify consistent and inconsistent states from unlabelled data. This is performed by giving an inconsistency score to each observation using the density factor for the *k*-nearest neighbours of the observation. An optimal inconsistency threshold is later computed to separate inconsistent from consistent observations. The second technique is based on a clustering-based proximity model, a fixed-width technique is used to extract proximity-detection rules that forms a small and most-representative data set for both inconsistent and consistent behaviours in the training data set. This is due to the fact that it is impractical to design SCADA-specific IDS detection solutions that retain all the training data since a large memory space is required and high computational costs are incurred when operating such solutions in the detection phase. The proposed solution uses a data-driven approach that does not require prior knowledge of the physical behaviour of the systems. This paper is organised as follows. It starts with an overview of SCADA-specific IDSs and discusses related works. Then, it describes the proposed solution. Finally, it summarises the main issues discussed in this paper.

The Proposed IDS-based SCADA Solution

This section discusses the proposed unsupervised anomaly-based intrusion detection solution, generating from unlabeled SCADA data, proximity anomaly detection rules based on the clustering technique. The solution is intended to monitor the inconsistent data behaviour of SCADA data points. It efficiently separates inconsistent from consistent observations in the learning dataset for multivariate data points; moreover, the proximity detection rules for each behaviour, whether consistent or inconsistent, are automatically extracted. In addition, the solution works in an unsupervised mode where “labeled" training data are not required; therefore, it does not require the involvement of an expert to extract detection rules. This will help to reduce time-expensive processing and eliminate human errors. Figure 1 shows the different steps of the proposed solution. First, the solution separates the inconsistent observations from the consistent ones in the unlabelled training data set, and an appropriate threshold is established to determine whether the observation is consistent or inconsistent. The fixed-width clustering approach is applied to extract proximity-detection rules which are used to detect inconsistent observations. The rest of this section illustrates each step in more detail.

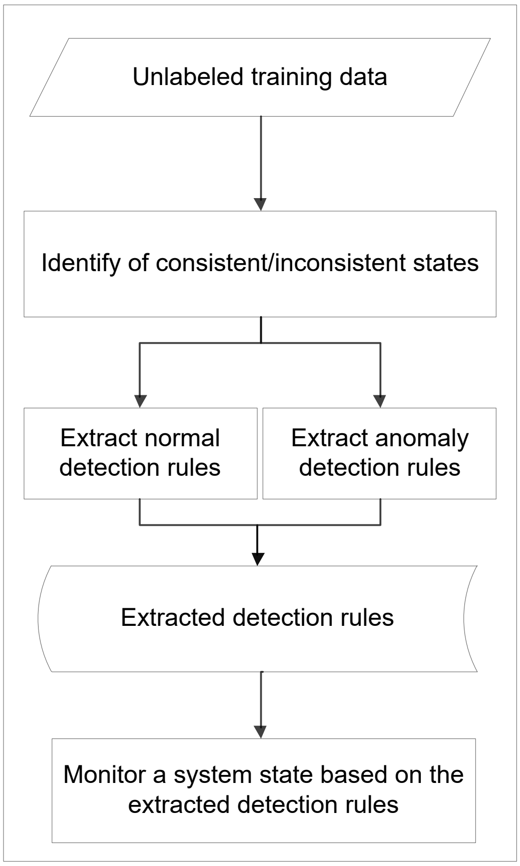

Unlabeled training data
Identify of consistent/inconsistent states
Extract normal detection rules
Extract anomaly detection rules
Extracted detection rules
Monitor a system state based on the extracted detection rules

Figure 1: the different steps of the proposed solution

- **A state of SCADA data:** The data of SCADA points such as sensors' readings and actuator control data, are data sources for the proposed IDS solution. The data consistency of SCADA points represents the normal current system state, while inconsistency indicates malicious actions. Consistent data are defined by the specifications that describe the valid data in terms of the system's operational perspective. The *state* can be defined as a combination of SCADA data produced by nodes at a certain period of time. States can be finite if the values of the nodes are discrete, or infinite when at least one of the node data is continuous.
- **Identification of consistent/inconsistent states:** The identification step, as illustrated in Figure 1, is the first phase in separating inconsistent SCADA data observations from the consistent ones. *A consistent state* is a state that statistically has the higher likelihood of being generated by the same mechanism that generated the majority of states. *An inconsistent* state is any state that statistically deviates from the majority of the states. To perform this step with unlabelled data, two assumptions are made: (i) the number of consistent SCADA data observations vastly outperform the inconsistent ones, and (ii) the inconsistent SCADA data observations must be statistically different from the consistent ones. Therefore, the proposed approach would be inappropriate for any situation that does not satisfy these two assumptions. The preliminary investigations show that inconsistent SCADA data observations have a similar definition of outliers in *n*-dimensional space and are sparsely distributed in an informal way. That is, they could take various densities of n-dimensional space. This is performed by giving *an inconsistency score* to each observation using the density factor for the *k*-nearest neighbours of the observation. Then, an optimal *threshold technique* is used to separate inconsistent from consistent observations.
  - *Inconsistency scoring***:** The proposed inconsistency scoring technique utilizes a hybrid of local and global outlier detection approaches. This is to ensure that the choice of the best approach should not be predominantly influenced by either local or global approaches. Therefore, the proposed inconsistency scoring technique relies on an average of distances of the nearest neighbours and the number of neighbours *k* that play a major role in the influence of local and

global approaches. To compute the inconsistency score for each observation, which is expected to consist of hundreds of dimensions, the cosine similarity metric is used, which can work with sparse numeric data and high-dimension space. This metric is used to measure the similarity between two vectors of n-dimensions, and it is widely used for clustering and information retrieval.

- *Threshold technique*: after assigning all observations with inconsistency scores, an appropriate threshold is essential to determine whether the observation is consistent or inconsistent. Thus, the selection of the near-optimal threshold is an important means of supporting the robustness of the inconsistency scoring technique, while an inappropriate threshold may lead to inappropriate results regardless of the criticality scoring technique. It is obvious that the labelling of consistent observations as inconsistent observations will result in a high false positive rate. Moreover, tuning the threshold to reduce the false positive rate is a critical operation because a number of true inconsistent observations may be missed. In the anomaly detection techniques that are based on anomaly-scoring, observations are sorted in descending order. Based on our assumption that consistent observations constitute a large portion of the training data set, they will also have very similar inconsistency scores. On the other hand, inconsistent observations are assumed to constitute a tiny portion of all observations, with high inconsistency scores, which are also assumed to be greater than the inconsistency scores for consistent observations.

Extracting proximity-detection rules: In fact, adding all the identified consistent and inconsistent observations into the IDS for monitoring is not a practical way because a large memory capacity is required to store all the observations. Thus, a detection rule extraction technique is proposed to extract a few detection rules which fully form the entire identified observations. As shown in Figure 1, detection rule extraction comes after the identification phase of consistent and inconsistent observations. During this phase, the fixed-width clustering technique is used to cluster each behaviour individually into micro-clusters with a constant fixed width, which is statistically determined. The centroids of all the created micro-clusters are used as the proximity-detection rules that are assumed to form a small and most-representative data set for both inconsistent and consistent behaviours in the training dataset. The detection rules are based on the mean of inconsistency scores of the states in the cluster with its centroid point and radius. The proximity-based detection rules are used to monitor any observation for the target system in order to assess whether the current observation is consistent or inconsistent. The evolution of SCADA data can reflect the system's state: either consistent or inconsistent. Therefore, the monitoring of the evolution of SCADA data for a given system has been proposed as an efficient tailored IDS for SCADA.

Conclusion

Intrusion Detection Systems (IDSs) have become an increasingly popular solution for anomaly detection in traditional IT. The increased importance of this solution has opened up an interesting research area in security, and its use is not confined to traditional IT, but has been adapted to detect unexpected behaviours in SCADA systems. However, the different nature and characteristics of SCADA systems have motivated security researchers to develop SCADA-specific IDSs. This paper discussed two innovative solutions that have been used together to make a robust unsupervised anomaly IDS for SCADA. The first solution involves the identification of consistent and inconsistent states from unlabelled data and the second one extracts proximity-detection rules for each behaviour, whether inconsistent or consistent. During the identification phase, the density factor for the k-nearest neighbours of an observation is used to compute its inconsistency score. Then, an optimal threshold technique is calculated to separate inconsistent from consistent observations. During the extraction phase, the well-known fixed-width clustering technique is extended to extract proximity-detection rules, which forms a small and most-representative data set for both inconsistent and consistent behaviours in the training dataset. In future work, we intend to dynamically update the extracted rules since the normal behaviours of a given system may evolve over time. In addition, the proposed solution will be evaluated with further intrusion-detection techniques for various application domains.

References

Boyer, S. A., 2009. *SCADA: Supervisory Control And Data Acquisition.* 4th ed. USA: International Society of Automation.

Slay, J. & Miller, M., 2007. *Lessons Learned from the Maroochy Water Breach.* Boston, International Conference on Critical Infrastructure Protection.

Falliere, N., Murchu, L.O. and Chien, E., 2011. W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), p.29.

Bencsáth, B., Pék, G., Buttyán, L. and Félegyházi, M., 2012, April. Duqu: Analysis, detection, and lessons learned. In ACM European Workshop on System Security (EuroSec) (Vol. 2012).

Yang, Y., McLaughlin, K., Littler, T., Sezer, S. and Wang, H.F., 2013. Rule-based Intrusion Detection System for SCADA Networks.

Munro, K., 2012. Deconstructing flame: the limitations of traditional defences. Computer Fraud & Security, 2012(10), pp.8-11.

Fovino, I.N., Carcano, A., Murel, T.D.L., Trombetta, A. and Masera, M., 2010, April. Modbus/DNP3 state-based intrusion detection system. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications (pp. 729-736). IEEE

Linda, O., Vollmer, T. and Manic, M., 2009, June. Neural network based intrusion detection system for critical infrastructures. In 2009 International Joint Conference on Neural Networks (pp. 1827-1834). IEEE.

Bhuyan, M.H., Bhattacharyya, D.K. and Kalita, J.K., 2013. Network anomaly detection: methods, systems and tools. IEEE communications surveys & tutorials, 16(1), pp.303-336.

Jin, X., Bigham, J., Rodaway, J., Gamez, D. and Phillips, C., 2006. Anomaly detection in electricity cyber infrastructures. Proceedings of CNIP.

Alcaraz, C. and Lopez, J., 2014. Diagnosis mechanism for accurate monitoring in critical infrastructure protection. Computer Standards & Interfaces, 36(3), pp.501-512

Rrushi, J., 2009. Composite intrusion detection in process control networks.

Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Fovino, I.N. and Trombetta, A., 2011. A multidimensional critical state analysis for detecting intrusions in SCADA systems. IEEE Transactions on Industrial Informatics, 7(2), pp.179-186.

Marton, I., Sánchezb, A., Carlosa, S. and Martorella, S., 2013. Application of data-driven methods for condition monitoring maintenance. CHEMICAL ENGINEERING, 33, pp.301-306.

Gao, W., Morris, T., Reaves, B. and Richey, D., 2010, October. On SCADA control system command and response injection and intrusion detection. In 2010 eCrime Researchers Summit (pp. 1-9). IEEE

Zaher, A.S.A.E., McArthur, S.D.J., Infield, D.G. and Patel, Y., 2009. Online wind turbine fault detection through automated SCADA data analysis. Wind Energy: An International Journal for Progress and Applications in Wind Power Conversion Technology, 12(6), pp.574-593.

An Evaluation of Phishing Email Awareness in an Information Warfare Age

Leon Hansan[1], Aaron Troiani[1], Patryk Szewczyk[1, 2]
[1]School of Science
[2]Security Research Institute
Edith Cowan University, Western Australia

Abstract. *This study investigated end-user awareness of contemporary phishing emails coupled with evaluating the success of specific scam types. In order to determine the ability of end-users to detect different phishing scams, an online survey was developed that required respondents to view ten emails and determine the authenticity. 83 respondents participated in the study between April and May 2019. 60 participants were unable to correctly identify a phishing email with a spoofed source email address. Respondents were also less proficient at identifying phishing emails when provided the opportunity to click on suspicious or unsafe links than they were at identifying emails with suspicious sender addresses.*

Keywords: Phishing, emails, end-users, network security, survey.

Introduction

Between January and September 2019, 16082 phishing scams were reported to Scamwatch Australia (Scam Statistics, 2019). From the reported phishing scams, 1.9% resulted in financial losses, totaling $891,556. While many end-users are aware of the existence of emails scams, the quantity of affected victims continues to increase (Parmar, 2012). Email scams are typically incentivized by offering the recipient a financial return, requesting urgent assistance or using scare tactics to encourage compliance (Williams & Polage, 2019). These approaches are successfully used to target home users and businesses (Burns, Johnson, & Caputo, 2019).

An effective technique to minimize an end-users susceptibility to email phishing scams is to reduce threat exposure by improving their overall awareness through education. Unfortunately, email phishing scams continue to increase in frequency and sophistication (Kirda & Kruegel, 2005). The methods used by scammers to construct phishing emails have becoming increasingly sophisticated whereby the typical victim struggles to differentiate phishing and authentic emails. Some of the methods being referred to include email spoofing, spear phishing, uniform resource location (URL) masking and malicious email attachments. Spear phishing is more concerning for organizations whereby employees are enticed or tricked through emails that appear to originate from an authoritative figure in the organization hierarchy. In a typical spear phishing attack, the email is constructed to look as though it has been sent from somebody inside the organization, which makes those types of emails further difficult to detect (Gupta et al., 2017).

Prior research into end-user phishing awareness has focused on evaluating the various factors that influence an end-user's susceptibility to be targeted. Research by Diaz, Sherman and Joshi (2018) indicated that students typically had a higher probability to be successfully exploited through phishing attacks. In contrast participants who are perceived to be extroverted are also more likely to fall victim to a phishing scam (Lawson, Crowson, & Mayhorn, 2018), whilst females within the 18 – 25 age group have also proven to be easily targeted (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). This paper focused on further exploring the email phishing techniques that are most effective at convincing participants of their authenticity, the techniques that are easier for participants to detect, and the varying degrees of success these might have across a range of age demographics; therefore, identifying what techniques are most likely to result in a successful attack.

Research Design

This ethically approved research was undertaken with participants who responded to an anonymous online survey. The survey consisted of ten email samples and asked respondents to identify whether they believed each email to be either phishing orientated or authentic. Of the ten emails that were provided, only two were authentic, while the remaining eight were phishing scams. In order to reduce ambiguity, some email samples were accompanied by a short description that provided context for the email (e.g. if the email was from a bank, the participant would be informed that they a customer of that bank).

Results

Between April and May 2019, 83 participants provided a completed response to the online survey. Participants were asked to rank their confidence from 1-5 with 5 representing a high level of cyber security confidence in contrast to 1 reflecting minimal or zero confidence. Table 1 shows the overall cyber security confidence levels amongst respondents in contrast to age.

Table 1 - Respondents Self-Evaluated Cyber Security Confidence

Age Group	**No. of Responses from each age group**				
	1	**2**	**3**	**4**	**5**
18 – 24			6	9	13
25 - 34			1	15	5
35 - 44		1	2	1	7
45 - 54		1	5	1	5
55 - 64			5	1	3
65 +			2		

Participants were further requested to rank their ability in detecting online scams. Table 2 shows each respondent's confidence in detecting online scams. This question used the same scale from 1-5 as previously shown and displayed similar trends throughout the age groups, with the younger participants displaying an elevated level of confidence and ability pertaining to cyber security.

Table 2 - Respondents Self-Evaluated Online Scam Detection Confidence

Age Group	**No. of Responses (Percentage from Each Age Group)**				
	1	**2**	**3**	**4**	**5**
18 – 24			7	14	7
25 - 34			8	9	4
35 - 44	1	1	1	3	5
45 - 54	1	1	4	5	1
55 - 64		1	4	4	
65 +		1	1		

Each respondent's self-perceived cyber security awareness was contrasted with correct responses from this study. Table 3 shows the correct, incorrect and unsure responses relevant to the respondent's computer confidence self-evaluation score. There were no major variations in the quantity of correct responses across the different score groups, only a very slight increase for those who rated themselves either a 4 or 5. There was also a slight decrease in unsure responses for these two groups, however the number of incorrect responses remained consistent.

Table 3 - Responses in Each Computer Confidence Self-Evaluation Group

Self-Evaluation Score (Phishing Detection Confidence)	**Percentage of Responses from Each Group**		
	Correct	**Incorrect**	**Unsure**
1	65%	25%	10%
2	53%	25%	23%
3	64%	25%	11%
4	67%	24%	9%
5	81%	14%	6%

Table 4 shows the correct, incorrect and unsure responses relevant to the respondent's self-evaluation of their ability to detect online scams. These results showed a reasonably consistent rate of correct responses, with a significant increase occurring (at least 13%) where respondents gave themselves a high rating of 5.

Table 4 - Responses in Each Online Scam Self Evaluation Group

Self-Evaluation Score (Computer Confidence)	**Percentage of Responses from Each Group**		
	Correct	**Incorrect**	**Unsure**
1			
2	65%	25%	10%
3	63%	22%	15%
4	69%	23%	7%
5	71%	22%	8%

Table 5 shows the correct, incorrect and unsure responses relative to each age group. There was no significant trend that followed these age groups for the correct or incorrect responses. However, there was a steady increase in unsure responses in the older age groups. This indicates that younger respondents were more confident in their answers, but not necessarily more accurate, and the older respondents were more likely to be unsure that they were able to correctly identify an email.

Table 5 - Responses in Each Age Group

Age Group	**Percentage of Responses from Each Group**		
	Correct	**Incorrect**	**Unsure**
18 – 24	64%	30%	7%
25 - 34	74%	18%	9%
35 - 44	75%	16%	8%
45 - 54	70%	18%	13%
55 - 64	59%	26%	16%
65 +	65%	15%	20%

Table 6 displays the total percentage of respondents that answered each question correctly, incorrectly and unsure. Most respondents (over 70%) were able to correctly identify the 2 authentic emails from the survey. Evidently, certain phishing emails had a reasonably high correct response rate (email 1, 6, 9 and 10), whereas others had a considerably lower correct response rate (email 2, 3 and 8).

Table 6 - Percentage of Correct Responses

Question Number	Percentage of Responses for Each Question			
	Question Type	Correct	Incorrect	Unsure
1	Phishing	86%	10%	5%
2	Phishing	41%	55%	4%
3	Phishing	51%	36%	13%
4	Phishing	77%	14%	8%
5	Authentic	88%	7%	5%
6	Phishing	78%	10%	12%
7	Authentic	72%	17%	11%
8	Phishing	28%	54%	18%
9	Phishing	78%	13%	8%
10	Phishing	83%	6%	11%

Table 7 outlines the phishing techniques that were used in each question on the survey. This information can be used to compare against the percentage of correct responses shown in Table 6, in order to determine what techniques are more likely to be effective.

Table 7 - Phishing Techniques Used in Survey

Email #	Techniques Used						
	Misleading Sender	Misleading Hyperlink	Generic/No Greeting	Misleading Contact #	Misleading URL	Unsafe Attachment	Spoofed Address
1	✓	✓	✓				
2		✓					
3	✓	✓					
4	✓			✓			
5							
6	✓		✓		✓		
7							
8					✓		✓
9	✓		✓			✓	
10	✓	✓	✓				

When comparing the results in Table 6 with the data in Table 7, it is evident that email #1 had a relatively high correct response percentage (86%) and made use of common phishing techniques (misleading sender address, misleading hyperlink and a generic/no greeting). However, email #8 had the lowest success rate (28%), even though the unsafe link was not hidden as a hyperlink, it was the only phishing email that used a spoofed email address. This may indicate that the respondents were not aware that email spoofing is possible and aren't paying as much attention to what they are being asked to click on, as they are the sender's email address.

Email #2 had the next lowest correct response percentage. This email was intended to emulate a spear phishing attack, so it was designed to look almost authentic, except for the hyperlink. Interestingly, of the 34 respondents that answered this question correctly, 16 incorrectly stated the senders email address as a reason for their selection. Again, this result indicates that respondents were focusing more on the where the email was coming from, then they were focusing on what they were being asked to click.

Email #3 was the third lowest scoring phishing email with only 51% of respondents correctly identifying it. While this email did contain a misleading sender address, it used the domain “google.support” in an attempt to convince respondents of its authenticity. This seemed to be effective, considering that of the 42 respondents that correctly identified the email, only 8 mention the email address as a reason for suspicion. Additionally, only 13 respondents, mentioned the contents of the hyperlink as being a cause for suspicion.

Except for email #3, the other emails that contained misleading email addresses were not particularly difficult to detect (all of these received over 75% correct responses). Most of these contained reasonably obvious spelling errors that respondents were able to detect. While these methods may be more effective in the real world, when people are not expecting to receive phishing emails, this research indicates that most people are able to detect fake email senders.

Conclusion

This survey has provided an insight into individual’s ability to detect email phishing scams and the various associated techniques. The results have indicated that there is a knowledge gap between the phishing techniques that are available and the techniques that average email users are aware of. This implies that there may be a need for increased email phishing education and awareness for end users.

As indicated from the survey results, email phishing scams that employ the use of spoofed email addresses were the least likely to be correctly identified by respondents. While users are aware of many commonly seen attributes of phishing emails (such as misleading sender email address or a generic greeting), it is somewhat clear that more technical approaches (such as a spoofed email address or spear phishing attacks) are easily overlooked by average users. Additionally, after reviewing feedback, respondents appear to focus heavily on the email sender, but significantly less on the hyperlinks and contents of phishing emails. This presents another area of technical naivety that may increase the chances of a successful email phishing attack. Therefore, it would only theoretically require an attacker to spoof the sender email address, in order to increase their chance of a successful phishing attack.

Surprisingly, there was minimal variance in the accuracy of the responses across different age groups. However, there was a higher percentage of unsure responses as the ages of respondents increased. This showed that a higher number of younger respondents were more confident in their responses, however, this did not translate to a higher number of correct responses, which was consistent with prior research conducted in this area (Sheng et al., 2010).

References

Burns, A., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. Journal of Organizational Computing and Electronic Commerce, 29(1), 24-39.

Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. arXiv preprint arXiv:1811.06078.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654. doi:10.1007/s00521-016-2275-y

Kirda, E., & Kruegel, C. (2005). Protecting users against phishing attacks with antiphish. Paper presented at the 29th Annual International Computer Software and Applications Conference (COMPSAC'05).

Lawson, P. A., Crowson, A. D., & Mayhorn, C. B. (2018). Baiting the Hook: Exploring the Interaction of Personality and Persuasion Tactics in Email Phishing Attacks. Paper presented at the Congress of the International Ergonomics Association.

Parmar, B. (2012). Protecting against spear-phishing. Computer Fraud & Security, 2012(1), 8-11.

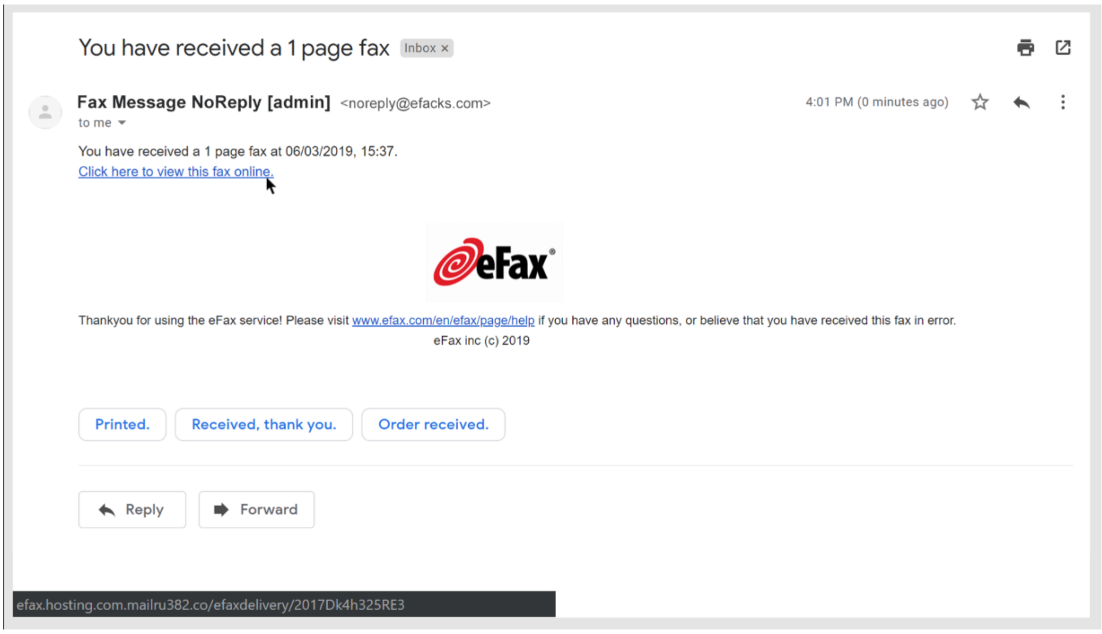
Scam Statistics. (2019). Retrieved from https://www.scamwatch.gov.au/about-scamwatch/scam- statistics?scamid=31&date=2019

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. Behaviour & Information Technology, 38(2), 184- 197.

Appendix – Phishing Emails

Email #1



You have received a 1 page fax

Fax Message NoReply [admin] <noreply@efacks.com>

4:01 PM (0 minutes ago)

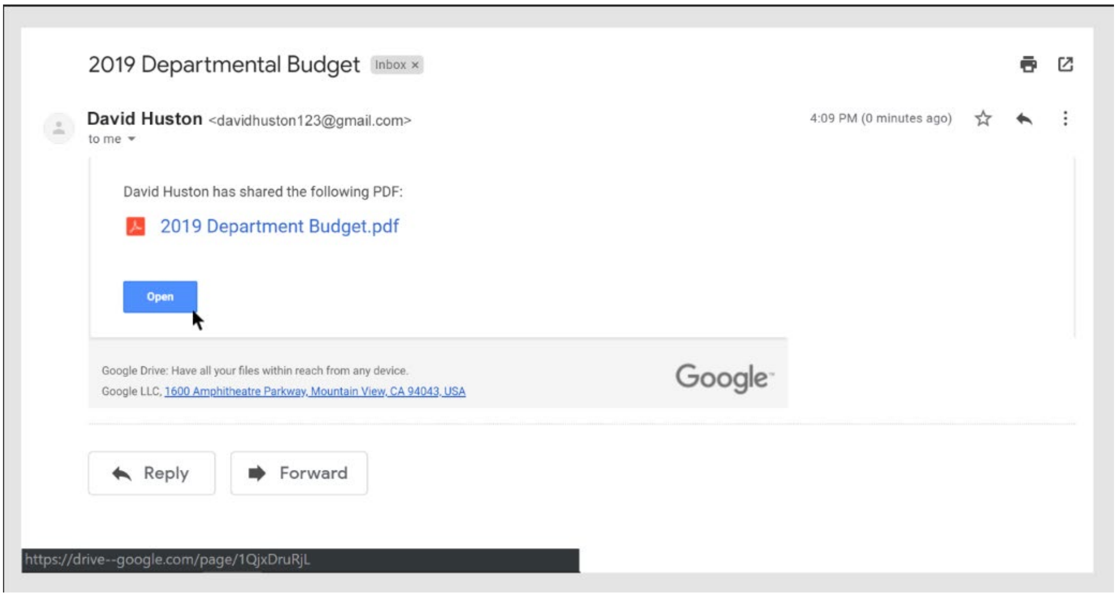
to me

You have received a 1 page fax at 06/03/2019, 15:37.
Click here to view this fax online.

Thankyou for using the eFax service! Please visit www.efax.com/en/efax/page/help if you have any questions, or believe that you have received this fax in error.
eFax inc (c) 2019

efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

Email #2



2019 Departmental Budget

David Huston <davidhuston123@gmail.com>

4:09 PM (0 minutes ago)

to me

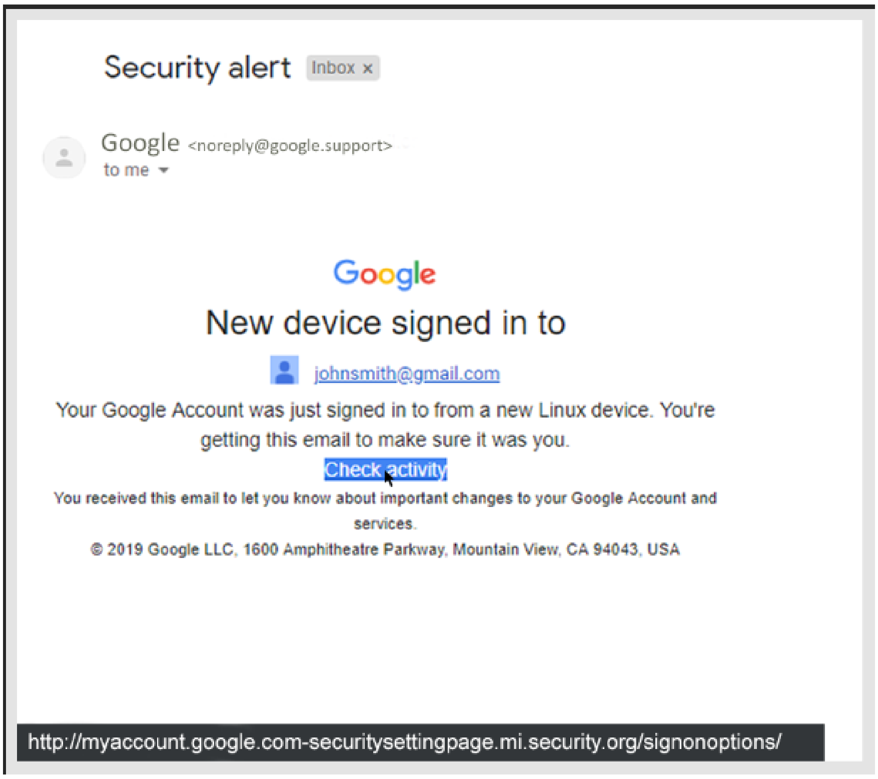
David Huston has shared the following PDF:

2019 Department Budget.pdf

Google Drive: Have all your files within reach from any device.
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

https://drive--google.com/page/1QjxDruRjL

Email #3



Security alert Inbox ×

Google <noreply@google.support>
to me

Google

New device signed in to

johnsmith@gmail.com

Your Google Account was just signed in to from a new Linux device. You're getting this email to make sure it was you.

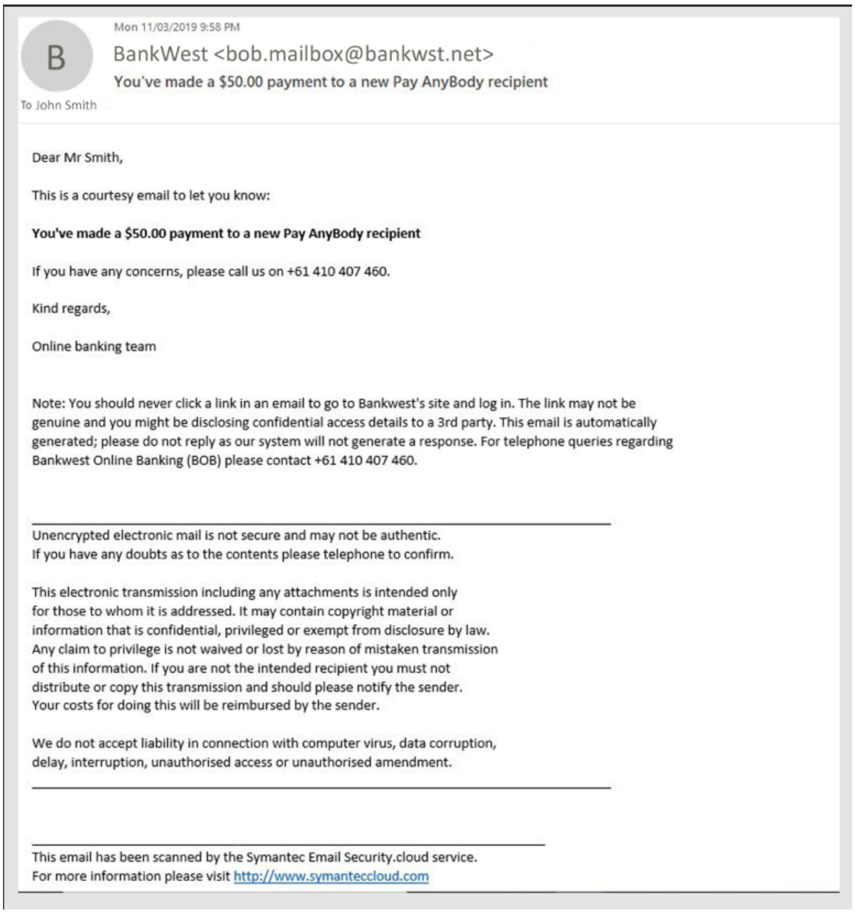
Check activity

You received this email to let you know about important changes to your Google Account and services.

© 2019 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

http://myaccount.google.com-securitysettingpage.mi.security.org/signonoptions/

Email #4



Mon 11/03/2019 9:58 PM
BankWest <bob.mailbox@bankwst.net>
You've made a $50.00 payment to a new Pay AnyBody recipient
To John Smith

Dear Mr Smith,

This is a courtesy email to let you know:

You've made a $50.00 payment to a new Pay AnyBody recipient

If you have any concerns, please call us on +61 410 407 460.

Kind regards,

Online banking team

Note: You should never click a link in an email to go to Bankwest's site and log in. The link may not be genuine and you might be disclosing confidential access details to a 3rd party. This email is automatically generated; please do not reply as our system will not generate a response. For telephone queries regarding Bankwest Online Banking (BOB) please contact +61 410 407 460.

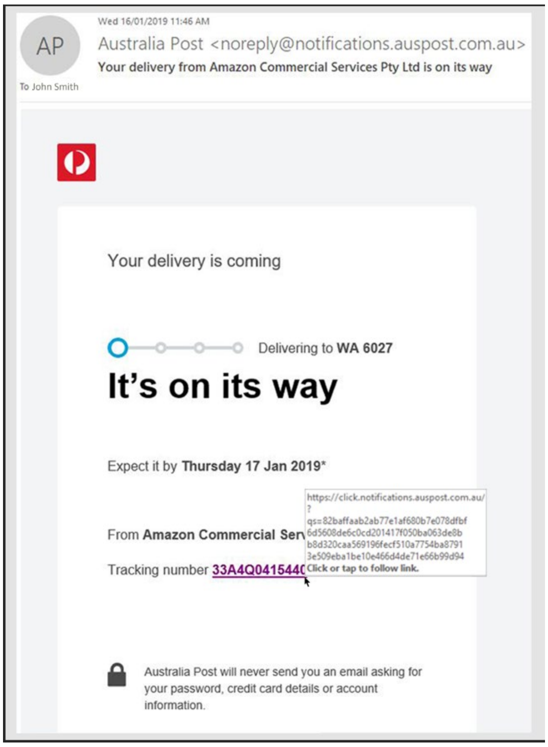
Unencrypted electronic mail is not secure and may not be authentic.
If you have any doubts as to the contents please telephone to confirm.

This electronic transmission including any attachments is intended only for those to whom it is addressed. It may contain copyright material or information that is confidential, privileged or exempt from disclosure by law. Any claim to privilege is not waived or lost by reason of mistaken transmission of this information. If you are not the intended recipient you must not distribute or copy this transmission and should please notify the sender. Your costs for doing this will be reimbursed by the sender.

We do not accept liability in connection with computer virus, data corruption, delay, interruption, unauthorised access or unauthorised amendment.

This email has been scanned by the Symantec Email Security.cloud service.
For more information please visit http://www.symanteccloud.com

Email #5



Wed 16/01/2019 11:46 AM

Australia Post <noreply@notifications.auspost.com.au>

Your delivery from Amazon Commercial Services Pty Ltd is on its way

To John Smith

Your delivery is coming

Delivering to **WA 6027**

It's on its way

Expect it by **Thursday 17 Jan 2019***

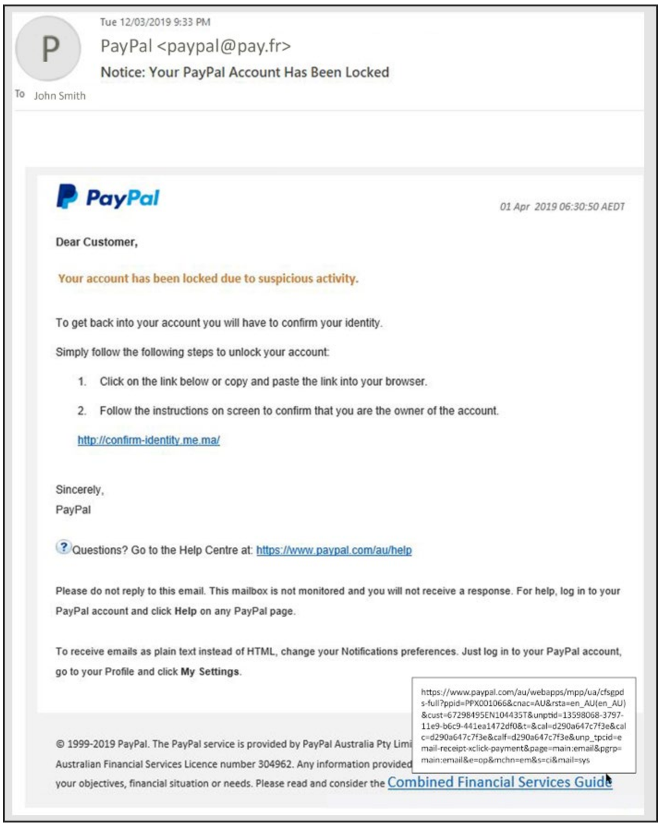
From **Amazon Commercial Serv**

Tracking number **33A4Q041544C**

https://click.notifications.auspost.com.au/
?
qs=82baffaab2ab77e1af680b7e078dfbf
6d5608de6c0cd201417f050ba063de8b
b8d320caa569196fecf510a7754ba8791
3e509eba1be10e466d4de71e66b99d94
Click or tap to follow link.

Australia Post will never send you an email asking for your password, credit card details or account information.

Email #6



Tue 12/03/2019 9:33 PM

PayPal <paypal@pay.fr>

Notice: Your PayPal Account Has Been Locked

To John Smith

01 Apr 2019 06:30:50 AEDT

Dear Customer,

Your account has been locked due to suspicious activity.

To get back into your account you will have to confirm your identity.

Simply follow the following steps to unlock your account:

1. Click on the link below or copy and paste the link into your browser.
2. Follow the instructions on screen to confirm that you are the owner of the account.

http://confirm-identity.me.ma/

Sincerely,
PayPal

? Questions? Go to the Help Centre at: https://www.paypal.com/au/help

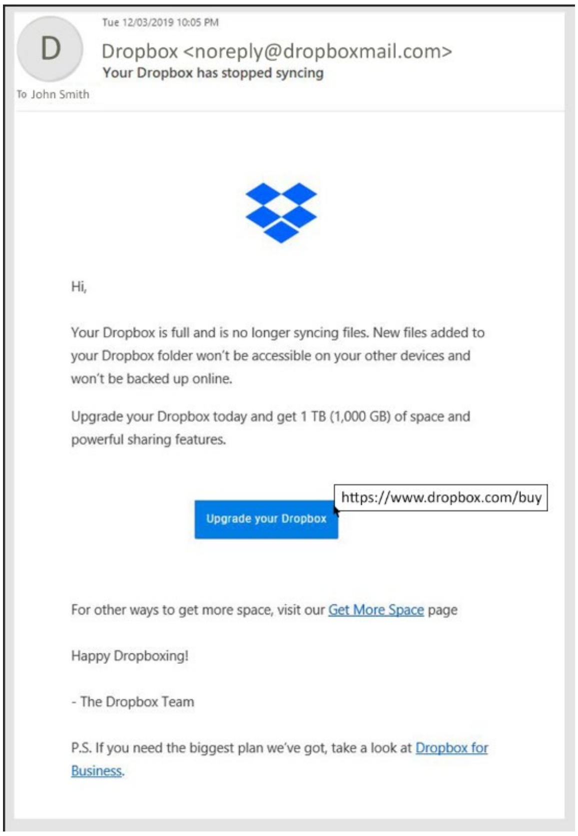
Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For help, log in to your PayPal account and click **Help** on any PayPal page.

To receive emails as plain text instead of HTML, change your Notifications preferences. Just log in to your PayPal account, go to your Profile and click **My Settings**.

https://www.paypal.com/au/webapps/mpp/ua/cfsgpd
s-full?ppid=PPX001066&cnac=AU&rsta=en_AU(en_AU)
&cust=67298495EN104435T&unptid=13598068-3797-
11e9-b6c9-441ea1472df0&t=&cal=d290a647c7f3e&cal
c=d290a647c7f3e&calf=d290a647c7f3e&unp_tpcid=e
mail-receipt-xclick-payment&page=main:email&pgrp=
main:email&e=op&mchn=em&s=ci&mail=sys

© 1999-2019 PayPal. The PayPal service is provided by PayPal Australia Pty Limi
Australian Financial Services Licence number 304962. Any information provided
your objectives, financial situation or needs. Please read and consider the Combined Financial Services Guide

Email #7



Tue 12/03/2019 10:05 PM

Dropbox <noreply@dropboxmail.com>

Your Dropbox has stopped syncing

To John Smith

Hi,

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

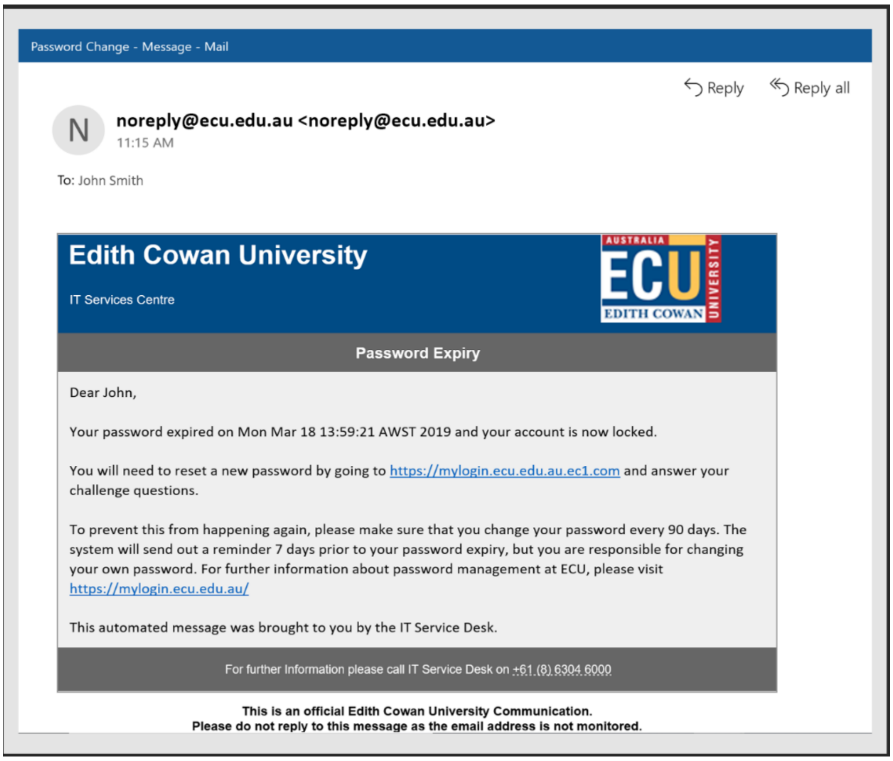
For other ways to get more space, visit our Get More Space page

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, take a look at Dropbox for Business.

Email #8



noreply@ecu.edu.au <noreply@ecu.edu.au>

11:15 AM

To: John Smith

Edith Cowan University

IT Services Centre

Password Expiry

Dear John,

Your password expired on Mon Mar 18 13:59:21 AWST 2019 and your account is now locked.

You will need to reset a new password by going to https://mylogin.ecu.edu.au.ec1.com and answer your challenge questions.

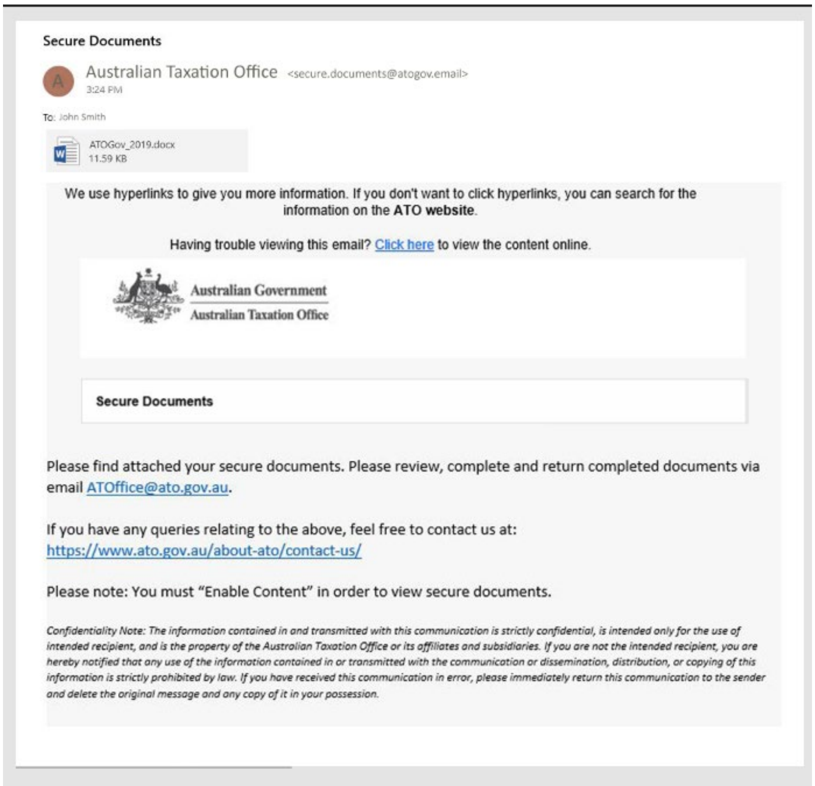
To prevent this from happening again, please make sure that you change your password every 90 days. The system will send out a reminder 7 days prior to your password expiry, but you are responsible for changing your own password. For further information about password management at ECU, please visit https://mylogin.ecu.edu.au/

This automated message was brought to you by the IT Service Desk.

For further Information please call IT Service Desk on +61 (8) 6304 6000

This is an official Edith Cowan University Communication.
Please do not reply to this message as the email address is not monitored.

Email #9



Secure Documents

Australian Taxation Office <secure.documents@atogov.email>
3:24 PM

To: John Smith

ATOGov_2019.docx
11.59 KB

We use hyperlinks to give you more information. If you don't want to click hyperlinks, you can search for the information on the **ATO website**.

Having trouble viewing this email? Click here to view the content online.

Secure Documents

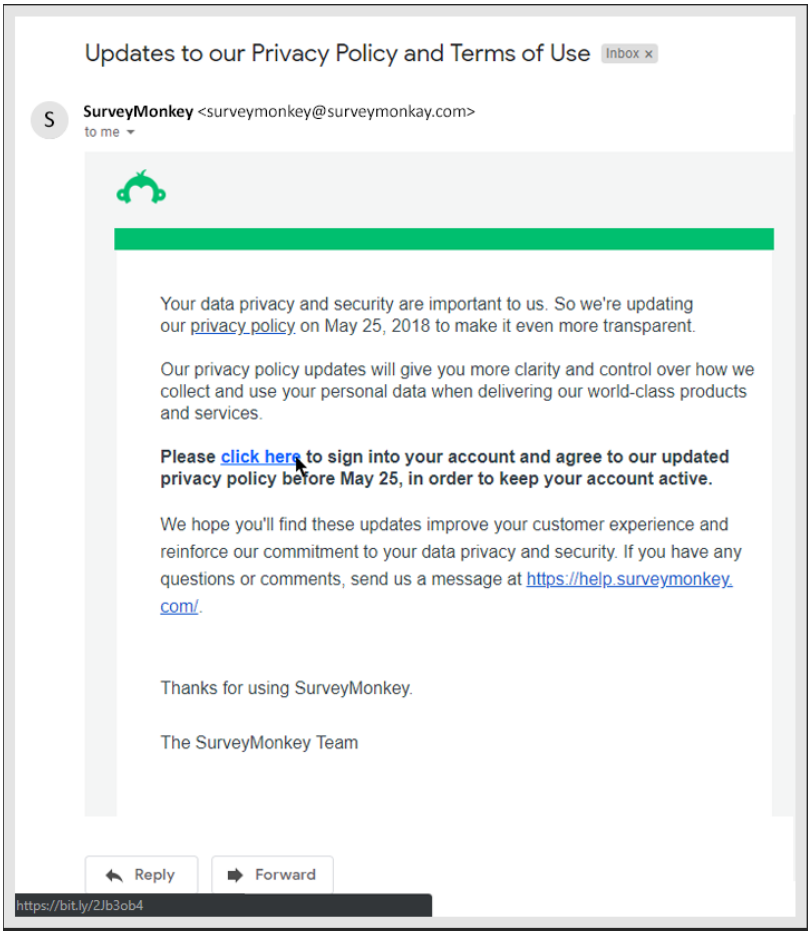
Please find attached your secure documents. Please review, complete and return completed documents via email ATOffice@ato.gov.au.

If you have any queries relating to the above, feel free to contact us at:
https://www.ato.gov.au/about-ato/contact-us/

Please note: You must "Enable Content" in order to view secure documents.

Confidentiality Note: The information contained in and transmitted with this communication is strictly confidential, is intended only for the use of intended recipient, and is the property of the Australian Taxation Office or its affiliates and subsidiaries. If you are not the intended recipient, you are hereby notified that any use of the information contained in or transmitted with the communication or dissemination, distribution, or copying of this information is strictly prohibited by law. If you have received this communication in error, please immediately return this communication to the sender and delete the original message and any copy of it in your possession.

Email #10



Updates to our Privacy Policy and Terms of Use

S

SurveyMonkey <surveymonkey@surveymonkay.com>
to me

Your data privacy and security are important to us. So we're updating our privacy policy on May 25, 2018 to make it even more transparent.

Our privacy policy updates will give you more clarity and control over how we collect and use your personal data when delivering our world-class products and services.

Please click here to sign into your account and agree to our updated privacy policy before May 25, in order to keep your account active.

We hope you'll find these updates improve your customer experience and reinforce our commitment to your data privacy and security. If you have any questions or comments, send us a message at https://help.surveymonkey.com/.

Thanks for using SurveyMonkey.

The SurveyMonkey Team

https://bit.ly/2Jb3ob4

Cyber Security Regulation. Assumptions for the Model of National Cyber Security Strategy

Darius Štitilis, Paulius Pakutinskas,
Marius Laurinaitis, Inga Malinauskaitė-van de Castel

Mykolas Romeris University, Ateities st. 20, LT-08303 Vilnius, Lithuania

E-mails: stitilis@mruni.eu; laurinaitis@mruni.eu (corresponding author).

Abstract: The task of ensuring cyber security plays an important role in national, regional and global security policies. The importance of this issue grows along with the increasing dependence of society on cyber space. The authors of this article analysed the existing regulatory situation on a higher level (on the scale of international, regional and national security strategies) as well as apparent trends; assessed the existing international regulation, its advantages and disadvantages, and national security strategies as well as their similarities and differences among them.

This article provides the evaluation of measures which could help achieve effective cyber security regulation, lists the considerations of whether the applicable international rules are sufficiently effective, what other measures could reinforce the fight against cyber threats or what unified cyber security strategies could be applied on a national level in individual states, and whether it would be an appropriate alternative for international legislation. This article presents a few surveys conducted by the authors, among them a qualitative survey on ten international cyber security experts' attitudes towards the existing regulatory situation in terms of cyber security.

Referring to the opinions of international cyber security experts, the authors of this article designed the main elements of the model of national cyber security strategy and put forward some suggestions as to which strategy components could be most unified and which should be intended for a better reflection of a national situation.

Keywords: Cyber security, cyber threats, cyber security strategy, cyber security regulation.

Introduction

Cyber security is defined as a cornerstone of information society (Schjolberg & Ghernaouti, 2011). The definition of cyber security has changed over the years (Craigen & Diakun, 2014) as follows:

2003
"Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders"

2006
" Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption."

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

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

2010
" The ability to protect or defend the use of cyberspace from cyber-attacks"

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

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

2014
"The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this."

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

The Oxford dictionary provides such definition of cyber security: The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this (The Oxford Dictionaries). More detailed definitions of cyber security may also be provided. For example, cyber security covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security) (ENISA, 2016). Differences in the definition of cyber security also exist in national legislation, despite the fact that cybersecurity has become a global phenomenon.

Recently most of the countries in the world have been increasingly focused on cyber security. The members of the EU and NATO are no exception. Cyber security is one of the most important priority areas in many states that aim at effective governance and assurance of continuous national and social processes as well as at the security of their citizens.

Despite the increasing effort put in ensuring cyber security, the level of cyber security in individual countries differs significantly. The differences (For example, differences related to legal foundations, operational entities, public-private partnerships, education, etc.) were shown in a BSA report (BSA, 2015). Research carried out reveals that the situation in terms of cyber security is different in the EU member states because of differences in the applicable cyber security strategies, requirements for cyber security audits, and incident reporting requirements (EU Cybersecurity Dashboard, 2015).

There are some EU, NATO, OECD and UN key documents influencing cybersecurity regulation. However, given the fact that, so far, no universally recognised imperative international initiatives have been developed which could in principle influence cyber security regulation, it could be stated that the development of international initiatives is at a relatively early phase and will have to evolve so as to generate satisfactory cooperation among the states in fighting against cyber security threats and to develop an international cyber security policy. The key steps are:

1. Methodology

In preparing this paper and presenting the outcome of research, their opinion and posture, the authors referred to the results of a few surveys. First, the authors examined international legal acts and factual situation related to cyber incidents. Second, the authors conducted a comparative analysis of cyber security strategies which enabled them to thoroughly examine and compare the provisions of the strategies. This research was made from all existing EU and NATO countries' national cyber security strategies.

Finally, a qualitative research also was carried out since a more profound analysis of the phenomenon required specific knowledge and experience of respondents. To analyse the models of cyber security strategies the best decision is to expert knowledge by employing the method of surveying experts' opinions as this helps accumulate the latest scientific knowledge. In this particular case, the authors interviewed experts of one specific level, i.e. they submitted their questionnaires to foreign experts asking them to complete the questionnaires in writing.

2. Analysis of International Regulatory Acts and the Factual situation Related to Cyber Incidents

The analysis of legal regulation on the international scale leads to the statement that currently there is no integrated and complex international legal act applicable in the area of cyber security. Reference could be made to the EBPO Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security of 2002 which is a non-binding act thus serves only as a recommendation. The content of this fairly old document is mainly related to the security principles which, in principle, withstood the test of time. Now the OECD Guidelines of 2002 are replaced by OECD 2015, Digital Security Risk Management for Economic and Social Prosperity. Certain national legislations clearly contain certain manifestations of these principles. Still, as pointed out in the Guidelines, they only suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security" (OECD Guidelines for the Security of Information Systems, 2001). In this way this document has more indirect effect and cannot be considered a regulatory act influencing the national law of states and at the same time the fight against cyber incidents. As regards binding international documents, the 2001 Council of Europe Convention on Cybercrime could be mentioned, however, this instrument is not intended directly for the field of cyber security but is rather designed for the harmonisation of criminal law and the law of criminal procedure in the field of cybercrime as well as the international cooperation and related aspects. Thus, it could be concluded that, in principle, there is no substantial legal regulation in the field of cyber security which would have an apparent direct impact on cyber incidents through corresponding national states.

One of the most efficient ways to coordinate the fight against cyber incidents and ensure cyber resilience is a national cyber security strategy. This type of document influences actions and efforts in single national jurisdictions. Significant differences in the strategies show that some interests, efforts and understanding of the issue in different countries can differ. The essential target to create a basis and an environment for cyber security in a country is unifying. Therefore, separate countries need to find unifying issues and to propose a cyber security model or international regulation. It has been a decade since the first cyber security strategies showed up in various countries around the world. Today, most countries have approved such strategies. Thus, regulation is developing by establishing and enforcing national documents. This article presents the analysis of how the national cyber security strategies help ensure a unified cyber security policy further below.

Regionally, situations are different. The US cyber security area is dominated by the self-regulation model. As Craig et al. put it, transition is needed to another type of regulation which would be aimed at improving cyber security in private sector by means of voluntary standards developed in similar industries (Craig, 2015). Meanwhile, in Europe, considerations could be made about unified cyber security regulation model based on legislation.

From the moment of establishment of the European Union, the field of cyber security was practically unregulated for many years. The first initiative was adopted only in 2013 when the EU approved the Cyber Security Strategy (Cybersecurity strategy of the European Union, 2013). The strategy sets forth the EU vision, explains the tasks and competences, points out the actions which should be taken. Still, the strategy is of general character and does not include all the components of a model of national cyber security strategy, and mostly focuses on cyber security principles and strategic priorities. Whilst the strategy was constructed to create a coherent approach, it is still evident that there is much to be done between the responsible national, regional and international institutions, networks and agencies to realise this. Besides, from the legal perspective, this strategy could be treated as a communication as it illustrates the EU's vision in the context of security strategy but is non-binding and the Member States are not obliged to take any specific measures.

At the same time this communication has also served as a way to submit the draft Directive on Security of Network and Information Systems. This draft was approved in 2016, when the first EU directive in the field of cyber security was adopted, namely, the NIS Directive (Directive on Security of Network and Information Systems) (Directive EU 2016/1148/EU). The aim of the Directive is to ensure a high common level of network and information security (NIS) across the EU (Directive 2016/1148/EU). Ensuring NIS is vital to boosting trust and to the smooth functioning of the EU internal market. Regulatory obligations are required to create a level playing field and to close existing legislative loopholes (European Commission, 2013). Provisions of the Directive had to be implemented in individual EU states from 9 May 2018. The Directive lays down the requirements for a national cyber security strategy, however, just like any other provisions these requirements will have to be legally applied from approximately July 2018. Thus, the tangible effect of the Directive will be seen solely after a few years. Moreover, the requirements of the NIS Directive for a national cyber security strategy are fairly short and fail to reveal a specific model of a national cyber security strategy.

These documents would seemingly suffice to develop the cyber security policy in a coherent and detailed manner and influence the unification of national cyber security strategies and the fight against cyber incidents; unfortunately, research and statistical data show a quite different situation.

Regardless of considerable effort and allocations, the number of cyber-attacks in the world is not falling (some surveys show a contrary trend), and the costs incurred by countries are dramatically increasing. Such leading countries as the USA, UK. Australia annually suffer increasingly big costs: the average annual cost of cybercrime in USA: 2017 – 21.22 USD millions, 2018 – 27.37 USD millions, in UK: 2017 – 8.74 USD millions, 2018 – 11.46 USD millions and in Australia: 2017 – 5.41 USD millions, 2018 – 6.79USD millions (The cost of cybercrime, 2019). Knowing that the aforementioned countries have substantial resources (both human and financial), an assumption can be made that weaker countries will be incapable of fighting against the growing cybercrime properly.

The rising number of cyber incidents is also confirmed by a number of other investigations: in UK 32% of businesses and charities 22% charities report having cyber security breaches or attacks in the last 12 months (Cyber Security Breaches Survey, 2019). Studies show that the total value at risk from cybercrime can reach even 5.2 trillion USD over the next five years (The cost of cybercrime, 2019).

Supposing that the number of cyber risks is continuously growing, their management by use of the existing regulation is ineffective. Besides, current laws and regulations appear to be much narrower in scope than the cyber security policies. This, in turn, requires new coordinated solutions and effective risk management methods. One of the most efficient ways to coordinate the fight against cyber incidents and ensure cyber resilience is national cyber security strategies. It has been a decade already since the first-second cyber security strategies showed up in various countries in the world. Today, most countries have approved such strategies. Thus, regulation is developing by establishing and enforcing national documents. The article presents the analysis of how the national cyber security strategies help ensure unified cyber security policy further below.

3. Differences Between National Cyber Security Strategies

A national cyber security strategy could be an instrument which determines a coordinated fight against cyber incidents and a tool used to protect information resources, including critical infrastructure. To find out what the situation in unifying national strategies in the field of cyber security is, the authors conducted surveys, i.e. a comparative analysis of strategies and a qualitative survey, namely, expert interviews by means of questionnaires.

The comparative research of the provisions of national cyber security strategies of EU and NATO Member States conducted by the authors of the paper has shown that the analysed strategies are very different. The main results of the comparative research revealed the following areas featuring differences in the content of the chosen national cyber security strategies: principles, cooperation with the private sector, international and research organisations, critical infrastructure protection, law enforcement issues, goals to fight cybercrime, cyber defence and its capabilities, cooperation, support of fundamental values/human rights.

First of all, the character of national security strategies should be addressed. Strategies of some countries serve more as documents which shape the vision in the field of cyber security (Strategies of Estonia, Spain, Austria, Germany, the USA, etc.). Meanwhile, cyber security strategies of some other countries are detailed and provide for an institutional structure, functions, responsibilities and even specific deadlines (Strategies of Cyprus, Luxembourg, Latvia, the Netherlands, the UK, etc.). Some states have adopted plans to implement the strategies which specify measures, the process of implementation, and the responsible entities in detail (Cyprus, Finland, etc.).

To detail specific differences discovered during the research on the strategies of the chosen states, it should be noted that the bigger part of the analysed strategies emphasises principles which are presented differently and that their number differs. More than 10 countries do not have separately distinguished cyber security principles in their national cyber security strategies. Some countries have 3 principles, while others have 13 and more. However, distinguished principles of the said countries have certain similarities: principles of proportionality, cooperation, the rule of law, responsibility, fundamental rights and freedoms, risk management and integrated approach are often distinguished. Still, despite of these similarities, there are many differences: certain countries divide principles into groups, in the strategies of other countries, principles themselves have distinguished subparts, unique principles are presented (such as the use of national products and services and increasing cyber force). Thus, the presentation of principles in national cyber security strategies of the examined countries can be stated to have no unified system, and despite some similarities, the principles differ.

Besides, the strategies are presented without any effort to have a unified system. Almost all of the analysed national strategies contain the aspect of cooperation with the private sector. However, the practical aspect of cooperation with the private sector is not implemented in all states, and in this way the provisions of these strategies remain declarative only.

Most often the fight against cybercrime or the reduction of the number of such crimes in the national strategies are singled out as a separate goal, milestone, challenge or principle. Also, it often happens so that national strategies have a separate strategy on fighting cybercrime or reducing the number thereof, discussing the issue and possible measures in greater detail. However, there were seven national strategies in which the fight against cybercrime was not pointed out at all.

The provisions of the chosen national strategies also considerably differ in terms of cyber defence and its capabilities. Twelve of the strategies do not address these issues at all, and the ones which touch upon this question present it as one of the goals or the main pillars. Some national strategies mention the aspect of cooperation with NATO in the context of defence. In assessing the cooperation with NATO in general, the analysed national strategies often mention it as an important element; however, it was not always referred to in the context of cyber defence. Besides, the strategies often mentioned the protection of critical infrastructure, but not always through the aspect of cyber defence. The importance of scientific research in the chosen national strategies is referred to in quite different contexts: either in relation to the necessity of the funded research or to cooperation with universities or schools.

A comparison of provisions in the support of fundamental values/human rights in national cyber security strategies has shown that the provisions of countries (a majority of them) which mention them are of a broader nature (related to human rights) or a narrower nature - perceived as support of privacy only. These values are often declared as one of the principles. Still, the strategies of 8 countries (Albania, Belgium, Cyprus, Denmark, Germany, Hungary, Luxemburg, Poland.) do not emphasize or mention the support of fundamental values/human rights, which is considered to be a rather large number of countries in light of the fact that remembering human rights and respecting them is very important in ensuring cyber security.

The issue of cooperation should be discussed separately. Cooperation is especially important in effectively resolving the international problem of cyber security that has no boundaries. The borders of the states are limited geographically, just like the administrative jurisdiction of countries. For this reason, national and international cooperation is considered the main tool for the effective fight against incidents. It is a cornerstone aspect on the basis of which the exchange of information on cyber incidents is coordinated. Good practices are shared and cyber defence actions are coordinated. Although cooperation is mentioned in the majority of cyber security strategies, cooperation as such is understood very differently; individual states stress, in principle, different levels, ways and agents of cooperation. Still, the major drawback is the fact that cooperation in most national strategies is described as a domestic process (taking place within the boundaries of the states), e.g., cooperation with the private sector, or cooperation with universities. Meanwhile, the strategies obviously lack the provisions on cooperation on the international and/or regional scale, and cooperation with international organisations (NATO, UN, etc.). There is a shortage of such explicit cooperation standards in national cyber security strategies and this might possibly negatively affect the fight against cyber incidents as well as the outcomes of such incidents globally.

In addition to above presented analysis, the experts pointed out the drawbacks of the strategies. They most often mentioned the shortage of the quality of a strategy's goals. However, it could not be stated that this was the prevailing drawback – experts listed fairly different areas. For instance, as drawbacks the following items were mentioned: insufficient consideration of such "secondary" sectors of the critical infrastructure as the field of healthcare, the absence of a relation with the main public goals, as well as irregular updates. Some strategies devoted more attention to the security of military facilities, objects and information systems, but much less to the issue of how to strengthen law enforcement capacities and how to support science in order to build new tools for public awareness. In addition, one expert specified the following problem: adopting a strategy without allocating resources for implementing the decision.

Evidently, the aforementioned differences and drawbacks affect the implementation of each of the analysed national strategies. Some states stress the critical infrastructure, whilst others the cooperation with NATO, education and research institutions or other organisations. In this way, cyber security priorities are different and are determined in different ways. Thus, the variety of the contents of the national cyber security strategies raise a number of thoughts in regard to the differences of the provisions, the crystallisation of common cyber security priorities and the effectiveness of implementation of such strategies. Even an analysis of cyber strategy reveals a broad divergence in approaches to cyberspace (Kshetri, 2013). In assessing the phenomenon of cyber security as a global issue which is relevant to all states, in the opinion of the authors, the need for a unified model of a national cyber security strategy should be considered or even several versions of model should be developed, given the specific particularities of different countries.

4. The Potentials of a Model of a National Cyber Security Strategy to Ensure Cyber Security

All the experts pointed out that the national cyber security strategy is really important and necessary for every state. However, different reasons were provided to support this statement. They illustrated that there is no single reason why the national cyber security strategy is important – these reasons may be related to the preparedness to resist external cyber-attacks, identification of problems and solutions in the field of cyber security, etc. The divergence of reasons demonstrates that though the importance of the national cyber security strategy can be assessed via different dimensions; there is one common denominator, i.e. a better assurance of cyber and even national security. Perhaps a model of a national cyber security strategy could ensure such security? Scientific sources consider the idea of a unified strategy in separate areas, e.g., a unified strategy to fight cybercrimes (Kshetri, 2013). As well International telecommunication union (ITU) produced the Guide to developing a national cybersecurity strategy (Strategic engagement in cybersecurity, 2017). However, there are not enough considerations and discussions about a unified cyber security strategy.

First of all, the very phenomenon of cyber security is of global character. When analysing the cyber security phenomenon, researchers emphasise global cooperation and legal certainty (Craig, 2015). They suppose that global cooperation is practicable only when there are explicit and fairly similar rules of operation. Second, once the national cyber security strategies of the same model are established, the cooperation mechanism with international organisations, such as NATO, would become simpler and more effective. Cyber security could become the main NATO policy which would also set the level of importance of the strategic NATO provisions in cyber security (Carayannis, Campbel, Efthymiopoulos, 2014). It should be noted that the issues of cyber defence were intensively raised by NATO partners during the Warsaw Summit (Defence News, 2016). And thirdly, it is thought that as similar as possible national cyber security strategies would help ensure a common cyber security policy and foster the common cyber security culture in as equal manner as possible. The potentials of unification of national cyber security strategies could help avoid the inconsistence of cyber security policies as well as frequent contingencies in the field of cyber security. The unification of national cyber security strategies is possible only through a model of cyber security strategy.

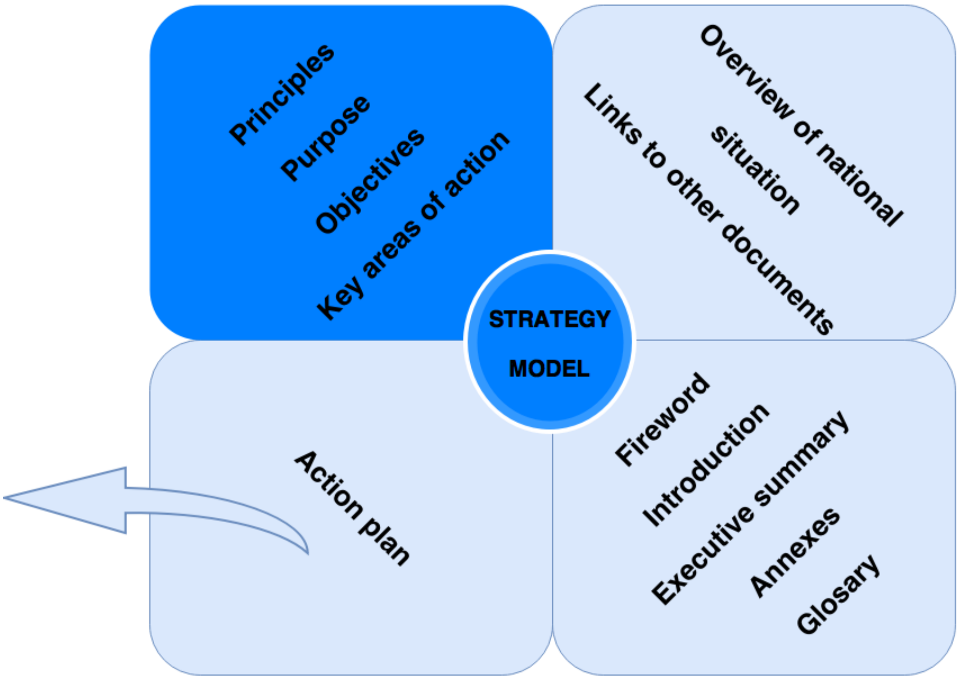
Yet, a question arises, whether a model of a national cyber security strategy must guarantee full unification of national strategies. National cyber security strategies may contain differences. The interviewed experts specified many different reasons suggesting why national strategies differ (e.g., different national needs, knowledge, capacity, budget, culture, economy, political and legal culture, political priorities, etc.) All in all, the substantiation referred to the differences among the states. A few reasons explaining the indicated differences could be mentioned:

countries differ in their military strategies, national security strategies, legal culture, culture on the whole, and political priorities. National cyber security strategies may also contrast in terms of the same aspects. One of the experts even pointed out that if a strategy fails to reflect national particularities, this should be considered a major drawback.

National cyber security strategies could be partially unified. However, some parts should be unique, e.g., the relation to other documents in a particular country. Some other parts of corresponding strategies could also contain certain differences. Perhaps a model of a strategy should have the obligatory parts and also leave some room for the establishment of national specificities which are essential and must be reflected in the strategy (e.g., the geopolitical status).

The provision of a specific and detailed model of a national cyber security strategy is an issue of a separate publication which requires a separate independent research and analysis. Nonetheless, referring to the surveys carried out, the authors outline such model further in this paper[1]. The contours of the model will probably contribute to further discussions and research on this issue. Figure No. 1 provides a graphical model of a national cyber security strategy. Based on the results of the comparative analysis and the opinions of experts, the authors suggest unifying these areas of the model of national cyber security strategy (dark blue means that these parts should be mostly unified, and bright blue implies that in such cases national aspects should play the major role):

Figure No. 1. Areas of the Model of a
National Cyber Security Strategy.
Designed by the authors.



The unified aspects of the proposed national cyber security strategy shall include principles, purposes, objectives and key areas of action. These four aspects were indicated as fundamental and core universally by the experts. Therefore, they might be referred in all cyber security strategies. Other elements of the proposed cyber security strategy shall include aspects, which are more linked to the particular country: an overview of the national situation, links to other documents, an action plan, a foreword, an introduction, an executive summary, annexes and a glossary. Each country shall draft the mentioned aspects in its own way and manner. It shall also be mentioned that the model of the national cyber security strategy is only a sketch, which might be developed by each particular country and may include other than in Figure No. 1 revealed elements.

The analysed problem of ensuring cyber security includes many areas of human activity and arises from technological changes, i.e. technology leads to the discussed security problems. However, it is not technology that poses the problems but rather people who exploit the capabilities of technology and apply them to achieve their goals, i.e. most of problems of other than technological character. They are the outcome of a man's relationship to technology and other people. Besides, the majority of issues are of a social nature, and they are analysed by the social sciences. For this these reasons, the principles of social sciences are used to tackle them. These may be the principles of law, management, economics, etc. The authors hold the view that the principles are of paramount importance in cyber security strategies as well. The principles in cyber security strategies can be thought of as generally accepted characteristics or expectations, but they also stress the need for a national effort, a preference for the reliance on market forces, and the importance of flexibility and multiyear planning (Fisher, 2009).

The inquired experts unilaterally pointed out that a national cyber security strategy must introduce principles. The experts singled out the following principles (in the order of their importance): Responsibility, Protection of fundamental rights, Cooperation, Openness, Privacy, Holistic approach and Availability. In determining the principles in strategies, there is no need to reiterate the universally accepted principles applied in other fields, for instance, law (supremacy of human rights, etc.), since the strategy cannot and has no purpose of annulling or replacing them, and they are applicable according to other national and international regulatory acts. It would be appropriate to establish not only special principles of cyber security strategies or principles which, in the context of cyber security, would acquire greater importance than in other areas of human activity. It is, however, important that the general or special principles incorporated in the strategy were truly fundamental for achieving cyber security; it is then likely that listing such principles in one document would result in a coherent system of principles.

Any meaningful framework for cyber security should include a clear description of its goals — the desired results or state (Fisher, 2009). The purpose and the objectives of a cyber security strategy constitute the basis both for the whole cyber security strategy and affect the state of cyber security in corresponding states. The experts marked the following goals of a strategy that should constitute the basis of a model of a cyber security strategy:

- Ensuring security in cyberspace by strengthening prevention, defence, detection and response capabilities;
- Strengthening the cyber security of critical national infrastructures;
- Raising the awareness of citizens, professionals, companies and authorities about the risks derived from cyberspace;
- Enhancing of the fight against cybercrime;

- Cooperating with international actors in order to achieve a consistent approach in strengthening cyber security.

The formulated goals lead to "key areas of action" which detail the goals and indicate more specifically as to where a state should focus in fighting against cyber incidents and ensuring cyber resilience. As the main areas, the experts singled out the following "key areas of action":

- Capability to prevent, detect, respond to and recover from cyber threats;
- Cooperation between the state and the private sector;
- Protection of critical information infrastructures (for example, identification, vulnerability assessment, penetration testing, contingency plan, etc.);
- National risk management system;
- Legal framework;
- Organisational structure (including roles and responsibilities);
- Training and capability development;
- Security culture (education, awareness);
- Cyber security research (including scientific).

In developing a unified national cyber security strategy, certain good practices should be used. The experts listed a number of useful good practices: cooperation, good incident reporting, standards, cooperation between the public and private sectors, awareness, development, etc. The aforementioned good practices can be taken from the cyber security field of corresponding countries where they are well developed or even from other related areas in corresponding countries, e.g., privacy protection. Privacy protection is very important from the General Data Protection Regulation (GDPR, 2016) perspective. The regulation, which comes into force on May 25, 2018, sets new standards for privacy protection and those standards should be highlighted in cyber security strategies as well. Also, the experts highlighted the importance of the cooperation aspect and listed other significant sectors which need cooperation: banks, insurance and finance sectors, healthcare, telecommunications, retail, energy, cyber technology, educational institutions, etc.

National security standards could be described in "Overview of national situation" and references to national security standards could be provides in "Links to other documents". Thus, the latter part should contain systematic references not only to national security laws, strategies and regulations but also to national security standards.

Additionally, a unified model of a cyber security strategy should be based on such traditional elements as a risk based approach, i.e. prioritization/mitigation actions on areas with the most risks, including a function based approach, and focus on resilience as a key element in a strategy to ensure that unexpected events can be handled and key/critical operation can be sustained.

However, the future trends for national security development, in the opinion of the authors, requires unification not only cybersecurity strategies, but also calls for unified cyber security policies as well, including cybersecurity laws and other regulations. Only by unifying cybersecurity policies of different individual states the resistance to global cyber security threats can be achieved. And we should consider not only regional unification, but also international unification of cybersecurity policies.

Conclusion

Most international documents are not imperative in matter. Therefore, international rules are insufficient to effectively tackle the problems related to cyber security and do not ensure sufficient coordination, especially at the strategic level. Despite the newly adopted Directive EU 2016/1148 of the European Parliament and of the Council of 6 July, 2016 concerning measures for a high common level of security of network and information systems across the Union, other effective measures to ensure the common effective fight against global cyber security threats have to be searched for. Some regional or international documents are quite promising. Successful implementation of cyber security measures will gain from unified international and national legal regulation. The key issue for unification is to find what is common for countries and to use it for modelling the laws. Unified requirements can be set in regional or international documents to ensure faster and uniform implementation.

Regulation evolves while intensively developing national regulation and mainly cyber security strategies. A cyber security strategy is the fundamental document on which the basis of the national cyber security policy is developed. Some countries have adopted “second-generation”, even “third-generation” cyber security strategies whilst at the same time evolving national cyber security policies from the initial to a more developed level. However, there is no sufficient unification in the field of cyber security, especially cyber security strategies. The models of national cyber security strategies or individual issues of their content differ. No unified cooperation model has been found yet. The differences could be seen in the content of EU and NATO national cyber security strategies: cooperation with the private sector, international and research organisations, critical infrastructure protection, law enforcement issues, goals to fight cybercrime, cyber defence and its capabilities, cooperation, support of fundamental values/human rights. In this way, cyber security priorities are different and are determined in different ways. Thus, the variety of the contents of the national cyber security strategies raise a number of thoughts in regard to the difference of the provisions, the crystallisation of common cyber security priorities and the effectiveness of implementation of such strategies. This situation could lead to weak coordination, cooperation between states and weak defence from global cybersecurity threats.

Unification is possible by developing a model of a national cyber security strategy which could be a perfect tool for making cyber security strategies similar, thus seeking to coordinate common effort in fighting against cyber incidents. The proposed cyber security strategy model of the authors includes both unified aspects, which should be reflected in the national cyber security strategies of all countries and national aspects, which exclusively relates to the peculiarities of the country (e.g., relation to other documents, analysis of the national cyber security situation, etc.).

This article presents the areas of a model of a national cyber security strategy which could be considered the key elements of such a model and most of which should have clearly expressed national specificities. The elements of a model of a national cyber security strategy which could be mostly unified could be the following: principles, purpose/objectives and key areas of action. These components should be the basis of every national cyber security strategy and the main tool for the unification of national cyber security strategies.

The proposal regarding a cyber security strategy model could be also seen as a possibility to have an internationally agreed unified model for a cyber security strategy. Could this model be obligatory as an international legal act is the question for additional research. However, the minimum proposal would be to evaluate the possibility to have such a model as a recommendation for all countries. The existence of such a model could harmonise cyber security elements in national states and could strengthen the fight against cyber incidents at the global level. International harmonization and unification should also apply to all cybersecurity policies of individual countries.

REFERENCES

1. Bernadette Hlubik Schell, Clemens Martin, 2004, Cybercrime– A Reference Handbook Contemporary world issues. ABC-CLIO
2. Brasso B. Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories. Business Of Security, Executive Perspective. FireEye, Inc. 2016. https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html
3. BSA. (2015) EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, [http://cybersecurity.bsa.org/index.html]
4. Carayannis E.G., Campbel D.F.J., Efthymiopoulos M.P. (2014) Cyber-Development, Cyber Democracy and Cyber-Defence: Challenges, Opportunities and Implications for Theory, Policy and Practice. New York: Springer.
5. CCDCOE: Cyber Security Strategy documents [https://ccdcoe.org/strategies-policies.html]
6. Christou G. Cybersecurity in the European Union Resilience and Adaptability in Governance Policy. New York, Palgrave Macmillan, 2016.
7. Cost of Cyber Crime Study: Global. Ponemon Institute. Research Report. October 2015. http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states
8. Craig N. A. et al. (b), Proactive cybersecurity: a comparative industry and regulatory analysis., American Business Law Journal, 2015.
9. Craig, Amanda and Shackelford, Scott and Hiller, Janine S. (a) Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis (March 4, 2015). American Business Law Journal, 2015. Available at SSRN: http://ssrn.com/abstract=2573787
10. Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, JOIN/2013/1 final. Brussels, 2013. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>
11. Daniel E. Geer, "Cybersecurity and national policy" Harvard National Security Policy. Vol. 1. 2010: 207-219.
12. Defence News. NATO Weighs Making Cyber Wartime Domain, 2016. http://www.defensenews.com/story/defense/2016/06/02/nato-cyber-warsaw-summit/85289290/
13. Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
14. ENISA 2012. ENISA Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace, 2012. https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

15. ENISA 2014. ENISA An evaluation Framework for National Cyber Security Strategies, 2014. https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport
16. ENISA 2016. ENISA NCSS Good Practice Guide Designing and Implementing National Cyber Security Strategies, 2016. [https://www.enisa.europa.eu/publications/ncss-good-practice-guide]
17. ENISA map. ENISA National Cyber Security Strategies (NCSS) online map [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map]
18. Definition of Cybersecurity - Gaps and overlaps in standardization. July 01, 2016. ENISA
19. EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace. BSA (Business Software Alliance), 2015, http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
20. European Commission. (2013). Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM (2013) 48 final. Brussels, 7 February, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666, accessed 1 February 2016
21. Fisher E.A. Creating a national framework for cybersecurity: an analysis of issues and options. New York, Nova Science Publishers, 2009.
22. GDPR, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
23. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf
24. ITU 2011. ITU National Cyber Security Strategy Guide, 2011. [http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
25. Jardin E. Global space is safer thank you think: real trends in cyber crime. Global commission on internet governance. Paper series: No. 16 – July 2015. https://www.cigionline.org/sites/default/files/no16_web_3.pdf
26. Johnson T.A. Cybersecurity: Protecting Critical Infrastructures from Cyber Attacks and Cyber Warfare. Taylor & Francis Group, 2015. ISBN: 978-1-4822-3923-2.
27. Klimburg A. National Cybersecurity Framework Manual. – NATO CCDCOE, 2012. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
28. Kshetri N. Cybercrime and Cybersecurity in the Global South. New York, 2013.
29. Ritchie J. ir Lewis J. Qualitative Research Practice: A Guide for Social Science Students and Researchers. Sage, 2003. P. 153-169.
30. Lemieux F. Current and Emerging Trends in Cyber Operations. New York, Palgrave Macmillan, 2015.
31. Meola A. Cyber attacks against our critical infrastructure are likely to increase. Business Insider. 2016. http://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5
32. OECD Guidelines for the Security of Information Systems: Towards a Culture of Security. Organization for Economic Co-operation and Security, 2001. https://www.oecd.org/sti/ieconomy/15582260.pdf
33. Schjolberg S., Ghernaouti-Hele S. A Global Treaty on Cybersecurity and Cybercrime. Geneva, 2011 (Schjolberg & Ghernaouti, 2011).

34. Štitilis D., Pakutinskas P., Malinauskaitė I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis // Security Journal, October, 2016
35. Tiirmaa-Klaar H., et. al. Bootnets. London, Springer, 2013.
36. Ventre D., Chinese Cybersecurity and Defense. London, John Wiley & Sons, Inc, 2014.
37. Wagner D. The Growing Threat of Cyber-Attacks on Critical Infrastructure. The Huffington Post. 2016. http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html.
38. Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. Defining Cybersecurity. Technology Innovation Management Review. October 2014 (Craigen & Diakun, 2014).

REVISITING SYRIA: CYBER OPERATIONS AS A MEANS OF HYBRID WARFARE

MEREDITH JONES AND SASCHA DOV BACHMANN

> "Over time, this conflict has exhibited all possible guises of war: civil war, proxy war, siege warfare, cyber-warfare and war against terror. All forms of past and present warfare seem to converge in this one conflict. A war against children, against hospitals, against cities, against first-aid workers, against memory, against justice – maybe these are more accurate titles for this war."[1]

INTRODUCTION

Modern warfare and the domains in which are classified as battlespaces continue to evolve alongside the weapons and technologies employed during conduct of hostilities. The Syrian conflict is no exception to this evolution and has often been a focal point of academic debate regarding the evolution of warfare. The Syrian conflict is one that has become increasingly complex due to the large range of contending parties that include both State and non-State actors. Notably, the extent of this conflict has travelled far beyond the borders of Syria, with the millions of displaced persons being the most apparent consequence.

This discussion paper captures parts of a larger project dedicated to the exploration of Syria as a hybrid war. It is the position of this discussion paper, and the overall project, that Syria is both: a conflict employing all strategies contained within the hybrid warfare classification as well as others from the full spectrum classification namely, irregular warfare, asymmetric warfare, and increasingly compound warfare. Before this backdrop, this discussion paper will explore the cyber operations that have been employed during the Syrian conflict and have been employed across the all domains and spectrums of the conflict.

HYBRID WARFARE – WHAT'S IN A NAME?

Throughout the course of hybrid warfare's evolution, a consistent definition has yet to be agreed upon, yet numerous scholars have discussed what is generally involved, with many overlapping in content. It has been argued, that hybrid warfare may display elements from existing categories of warfare, including irregular warfare (terrorism and counter-insurgency),

[1] Vincent Bernard, 'Editorial: Conflict in Syria: Finding Hope Amid the Ruins' (2017) 99(3) *International Review of the Red Cross,* 865, 865.

asymmetric warfare, and compound warfare.[2] Added to these could be the element of legal ambiguity as a consequence or objective of hybrid warfare reminiscent of the emerging trend of ‘grey zone’ tactics. A number of commentators have defined hybrid war, however, it has well-stated by Wilkie, that hybrid warfare is a conflict, “*in which states or non-state actors exploit all modes of war simultaneously by using advanced conventional weapons, irregular tactics, terrorism, and disruptive technologies or criminality to destabilize an existing order*”.[3] Throughout the evolution of hybrid warfare, several military components have emerged with two of particular importance for the purposes of this discussion paper; the increase of information warfare through cyber warfare, and the transition towards greater use of cyber and air-space domains. Within the context of hybrid warfare it has become clear that the use of cyber serves both as an enhancer of such warfare and possibly as a category on its own, namely below the threshold operations within the emerging cyber war/ conflict paradigm. To that end, the conflict in Syria has become one where previously untested battlefields and operational domains, have been explored and exploited.

SYRIA: CYBER OPERATIONS AS A METHOD OF ASYMMETRIC WARFARE

Asymmetric warfare, plainly said, is where the conflicting parties have a disparity between their capabilities, and as noted by Geiß, perfect symmetry between conflicting sides hasrarely been witnessed in times of war.[4] In contemporary conflicts, asymmetric warfare has been regularly employed within urban environments where militarily weaker parties do not often engage in conventional warfare tactics.[5] Despite the barrage of direct offensive strategies conducted by militarily strong parties, those who are weaker in capabilities are left to employ indirect offensives. These weaker parties are left to conduct “indirect offensive and defensive strategies such as guerrilla warfare, concealing themselves among supportive civilian populations in cities, towns, and villages, which provide both cover for them to launch attacks

[2] Ibid, 66.

[3] R. Wilkie, ‘Hybrid Warfare – Something Old, Not Something New’, Air & Space Power Journal 2009, https://www.airpower.au.af.mil/airchronicles/apj/apj09/win09/wilkie.html (last accessed 1 June 2016); Andres B. Munoz Mosquera and Sascha Dov Bachmann, ‘Lawfare in Hybrid Wars: The 21st Century Warfare’ (2018) 7 *Journal of International Humanitarian Legal Studies* 63, 66.

[4] Robin Geiß, ‘Asymmetric conflict structures’ (2006) 88 *International Review of the Red Cross* 757, 758.

[5] Michael John-Hopkins, ‘Regulating the conduct of urban warfare: lessons from contemporary asymmetric armed conflicts’ (2010) 92 *International Review of the Red Cross* 469, 470.

and also protection from counter-attack".[6] As stated by Adhami, cyber operations have been employed as guerrilla-style warfare to regain symmetry between parties.[7]

When analysing the presence of asymmetric strategies in modern warfare, the complicated conflict in Syria is by no means an exception, as there has been an obvious disparity between warring parties. Grohe concludes that the cyber operations conducted during the Syrian conflict have been 'more important than one might have expected'.[8] This conclusion is based upon research and data pointing to numerous actors involved in the Syrian conflict who have used cyber operations as a method of warfare. Such conduct has been evidenced by Iran, Hezbollah and the Syrian Electronic Army (SEA) in distributing propaganda, with the objective of disinformation and deterrence.[9] Unfortunately in the case of Syria, and as will be illustrated in the discussion below, rebel groups and anti-Assad combatants have not enjoyed the same ability to engage in cyber operations as a means of asymmetric warfare.

Cyber operations and capabilities can be far reaching and are often not confined to computer-based attacks. However, two schools of thought have emerged, each discussing the scope of 'cyber operations' within in a conflict situation. It is not the purpose of this discussion paper to make a determination as to which school of thought should be adopted, however discussion will take place around each.

The first school of thought takes a narrow interpretation that argues that cyber operations are generally constrained to computer-based attacks. To provide an example; throughout the Syrian conflict, Iran has tested their cyber-capabilities with attacks targeting armed opposition and at elements that extend to other operational domains.[10] Many of the cyber operations conducted by the Syrian regime were improved and expanded by Iran and Hezbollah, with numerous attacks being documented throughout the conflict.[11] Many of these cyber operations have been aimed at social media, foreign media outlets, and in some cases universities, with the main

[6] Michael John-Hopkins, 'Regulating the conduct of urban warfare: lessons from contemporary asymmetric armed conflicts' (2010) 92 *International Review of the Red Cross* 469, 471; Ivan Arreguın-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict* (Cambridge University Press, 2008) 4.

[7] Wael Adhami, 'The strategic importance of the Internet for armed insurgent groups in modern warfare' (2007) 89 *International Review of the Red Cross* 857, 868.

[8] Edwin Grohe, 'The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict' (2015) 32(2) *Comparative Strategy*, 133, 133.

[9] Marcin Andrzej Piotrowski, '"Mosaic Defence:" Iran's Hyrbid Warfare in Syria 2011-2016' (2017) 3 *The Polish Quarterly of International Affairs* 18, 21.

[10] Ibid, 28.

[11] Marcin Andrzej Piotrowski, '"Mosaic Defence:" Iran's Hyrbid Warfare in Syria 2011-2016' (2017) 3 *The Polish Quarterly of International Affairs* 18, 64; Edwin Grohe, 'The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict' (2015) 32(2) *Comparative Strategy*, 133, 136.

objective of disseminating propaganda and, as retaliation against the West.[12] Further, some operations have reportedly had the primary objective of obtaining operational intelligence on the battlefields in Syria.[13]

The broader school of thought argues that cyber operations extends to remote warfare, with unmanned aerial vehicles (UAVs) such as drones, at the heart of the argument.[14] The use of UAVs has been well-documented in Syria. Iranian drones have reportedly been used for reconnaissance, artillery direction and directs attacks.[15] Despite little affirmation as to their military operations in Syria, Israel has recently claimed to have carried out a drone strike to prevent further drone attacks by Iran.[16] Another major actor in the Syrian conflict, Russia, has also allegedly engaged in cyber operations which have included the use of UAVs and "ground systems to conduct electromagnetic reconnaissance and jamming against satellite, cellular and radio communication systems along with GPS spoofing."[17] The extent of Russia's operations, has been estimated to include more than 23,000 flights conducted by UAVs.[18]

CONCLUSIVE REMARKS

The Syrian conflict is one where previously untested battlefields and operational domains, have been explored and exploited. Although this conflict falls within the scope of hybrid warfare more broadly, this discussion paper has focussed on cyber operations as an asymmetric strategy. Within Syria, cyber operations continues to play a large role within the conflict. Despite mentioning that symmetry can be regained with the use of cyber operations, the same cannot be said in Syria. Due to the involvement of numerous actors participating in the hostilities, with several assisting the Syrian regime, asymmetry has been amplified between the warring parties. The examples provided in the above discussion does not by any means cover the extent of cyber operations within the Syria conflict. However, it aims to provide insight as to how cyber operations have been employed to enhance operational and strategic objectives in what seems to be a conflict with no end.

[12] Piotrowski (n 9) 39.
[13] Ibid.
[14] Emily Crawford, *Identifying the Enemy* (Oxford University Press, 2015) 126.
[15] Piotrowski (n 9) 34.
[16] 'Israel says it struck Iranian 'killer drone' sites in Syria', *BBC News* (online, 25 August 2019) <https://www.bbc.com/news/world-middle-east-49464546>

[17] Col. Liam Collins, 'Russia Gives Lesson in Electronic Warfare' (2018) 68(8) *Army* 18, 19.
[18] David Oliver, 'Russia's Rapid UAV Expansion' (2019) 43(6) *Armada International* 8, 8.

BotNets in the Internet of Things: The Next Wave

Ashley Woodiss-Field and Michael N. Johnstone
School of Science
Security Research Institute
Edith Cowan University
Western Australia
a.woodiss-field@ecu.edu.au, m.johnstone@ecu.edu.au

Abstract: *The Internet of Things (IoT) enables interconnectivity between (often) low-power devices to permit information exchange or environmental control. The explosion in popularity of IoT devices has meant that security has not been a principal requirement for IoT devices. This is particularly true for botnets, where a remote threat actor could control IoT devices. We examine the fundamentals of botnets and how they are detected. Our contribution is to examine two conventional botnet detection tools and to suggest the likely success of botnet implementation in IoT network environments. We also tested the session replay component of BotProbe.*

Introduction

Similar to other network systems, an IoT network can be conceptualised as three layers. The hardware layer, which consists of sensors (i.e., networked devices), is responsible for data collection. The middleware layer stores data, performs analysis and makes decisions for an IoT network. The presentation layer is responsible for data visualisation and delivery (the latter may be to sources outside the network). The presentation layer may be instantiated as an API that can be used by other applications or possibly directly accessed by an end user, by some form of Human Machine Interface or HMI (such as a touchscreen). Unfortunately, as will be seen below, the type of mesh network that provides the transport, compute-power, scalability and redundancy for IoT networks maps very well to the architectures of botnet systems.

A botnet is a particular type of cyber security threat that works by infecting a group of machines and then using those machines to conduct cyber security attacks on another party (Woodiss-Field and Johnstone, 2018). It is thus a realisation of a threat that works by using compromised systems to perform a malicious action. A botnet will typically be comprised of IoT devices that have been infected in some way. Once sufficient devices have been added to the botnet, a threat actor can use the botnet to perform cyberattacks such as Denial of Service, spamming, phishing attempts, click fraud or illegal hosting. Botnets have several known architectures, but will usually be coordinated by a controller of some kind in a master-slave relationship.

Since the Mirai attack of 2016, research into botnets has been resurgent. Mirai was particularly interesting because of its sophistication, in that it used a federated model, not a simple controller-drone model.

Libicki (1995) proposed a taxonomy which included seven types of information warfare. It is type five, software-based attacks on information systems, which is of relevance to this work. Conceivably, types six and seven (information economic warfare or war via the control of information trade and cyberwar) might also be appropriate.

Hutchinson and Warren (2001) state that if the target is the data, then potential information warfare actions that could be undertaken include denial of access, disruption or destruction, theft or manipulation. All of these actions are feasible with a botnet.

In the following section we examine the benefits and drawbacks of two current approaches to botnet detection, viz., BotProbe and BotMiner.

BOTNET DETECTION

BotProbe is a botnet detection tool proposed by Gu, Yegneswaran, Porras, Stoll, and Lee (2009) which uses packet spoofing as an integral part of its detection approach. The premise that BotProbe operates on is that compromised systems that have become part of a botnet will respond to communications from the botmaster in a deterministic way. BotProbe extracts suspicious network traffic recordings and attempts to replay suspected bot commands to the suspected bot. After spoofing a potential bot command, the traffic produced from the bot is examined further and compared to previous recordings to determine if it demonstrates a consistent pattern of behaviour (Gu et al, 2009).

Among contemporary techniques examined, BotProbe, at least conceptually, appears to be among approaches potentially suitable for IoT-based bot detection. Internal host-based techniques are inadequate for low-powered devices and have had only limited success for traditional botnet detection (Stinson and Mitchell, 2007; Zeindanloo, 2010). Signature-based techniques cannot detect emergent threats and may not be able to detect modified strains of previously used malware (Liu, Xiao, Ghaboosi, Deng, and Zhang, 2009).

BotMiner may be suitable for some IoT-based botnets but depends on the premise that bots on the same botnet will propagate throughout entire networks (Gu, Perdisci, Zhang, and Lee, 2008). Mirai notably does not attempt to propagate on entire networks and due to the availability of IoT devices, other IoT-based botnet may be capable of following that model (Elzen and Heugten, 2017).

BotProbe is capable of single bot detection, does not utilise signatures, and does not need to be installed on the device itself. These factors mean that conceptually the BotProbe techniques may be capable of detecting IoT bots if adjusted correctly (Gu et al, 2009). Other techniques may also be suitable for IoT bot detection, such as certain DNS-based techniques or techniques that utilise signatures and event correlation (Choi, Lee, Lee, and Kim 2007; Gu, Porras, Yegneswaran, Fong, and Lee, 2007).

BotProbe first filters network traffic to only those that could potentially be botnet commands. In the tool as originally proposed, these filters apply to only certain IRC packets. Network traffic is then further examined by checking the potential bot's immediate activity after receiving communication. If it appears that the potential bot is enacting a command based on the timing and nature of the activity, the potential command, bot, and involved IRC server are examined further (Gu et al, 2009).

The session replay component of the BotProbe operates by recreating the suspected command packet and sending it to the potential bot. The response of the bot is then examined and compared to the original responses from the filtering phase (Gu et al, 2009). Other components of the BotProbe include:

- Explicit Challenge, a captcha sent to potential bots
- Session byte probing, similar to the session replay probing except that some bytes are modified
- Client replay probing, sending commands to potential bots via IRC as a botmaster would instead of replicating packets
- Man in the middle component, supplementary component designed to account for command obfuscation/modification by capturing ongoing suspicious communications and replaying them
- Multiclient probing, supplementary component for applying the BotProbe techniques to multiple suspected bots

For the purpose of experimentation, the initial filtering and session replay component of the BotProbe tool was recreated by closely follow the literature's specification. The session replay component was chosen as, among the proposed components, it could operate without directly interacting with an involved IRC server (Gu et al, 2009). IRC servers involved with botnet communications are often not malicious by design, instead unwittingly used for bot operations (Shanthi and Seenivasan, 2015). Isolating only the suspected bot also reduces the potential for unknown factors or conflicts during the probing process. For example, if the client replay component of BotProbe were to be used and the botmaster has a nick registered for CnC, the probe may not be able to join the session or the bot may not respond to a different nick.

During development of the BotProbe components, it became apparent that the filtering technique as proposed could only work on a specific protocol, in this case IRC. Engineering this part of tool could potential be applied to other protocols, however doing so dynamically may not be feasible. Peer to peer protocols, and other bespoke methods of communication, may be difficult to detect without overhead or the development of more advanced filtering techniques.

Once developed, the session replay technique was tested on a simulated IRC botnet. The probe was able to successfully determine the operating bots; however, the probe also caused the bot respond to a false communication. This unwarranted response caused the bot to drop its IRC session, disconnecting it from the botnet. This did not impact the detection as the bot activity still took place after receiving the spoofed command. However, if a legitimate IRC user became suspected as a bot by the filtering process, something the original BotProbe authors anticipated, it may lead to legitimate IRC sessions being dropped occasionally (Gu et al, 2009). While not necessarily applicable to non-IRC based scenarios, some consideration into further development may be required as the probe may have adverse effects on device and network functionality.

The BotProbe technique is limited by a constrained scope, in this case IRC, that may prove difficult to expand in a way that can confront emergent threats. The BotProbe technique also has the potential to disrupt legitimate services if they are subject to probing. The constraint may be remedied through developing a tool able to determine communication through means other than protocol filtering. Device and network functionality disruption may be mitigated through quarantine or alerting but developing such a method on an autonomous IoT network without affecting availability may not be possible. If the BotProbe technique were to be reengineered to probe different protocols dynamically as they are detected, the consequences of spoofing a range of communications may cause problems for certain types of networks. The technique would have to be deployed conscientiously, which may not be adequate in many scenarios.

Although limited by scope and potential disruptive results, especially if applied dynamically, BotProbe could potentially be reengineered for IoT-based bot detection if it were further supplemented. The literature states that the false positive rate for the technique is low and that it can detect certain bots after only one command has been sent through, assuming the that the command had been successfully carried out and that no obfuscation had been applied (Gu et al, 2009). Testing of the recreated BotProbe has appeared to have demonstrated that to be the case. If the shortcomings of the technique can be mitigated, a modified version of the BotProbe technique may prove capable of supporting IoT-based botnet detection.

Conclusion

It is unlikely that current approaches to botnet detection would have detected a sophisticated threat such as Mirai. Whilst Mirai used comparatively large IoT devices (for example, CCTV cameras), there is no evidence of smaller devices, such as temperature sensors, being used in this fashion as yet. Current approaches solve specific problems by being constrained to being deployed against a particular protocol (e.g., HTTP) or a particular transport application (e.g., IRC). Such approaches are problematic in an IoT space where devices use different, simpler protocols. More general solutions are still to be found, but it is likely that a data-driven approach using one or more machine learning algorithms could prove fruitful.

References

Elzen, I., & Heugten, J. (2017). Techniques for detecting compromised IoT devices (Master's thesis, University of Amsterdam). Retrieved from http://work.delaat.net/rp/2016-2017/p59/report.pdf

Gu, G., Perdisci, R., Zhang, J., Lee, W., et al. (2008). Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection. In: Usenix security symposium (Vol. 5, pp. 139-154).

Gu, G., Porras, P. A., Yegneswaran, V., Fong, M. W., & Lee, W. (2007). Bothunter: Detecting malware infection through ids-driven dialog correlation. In: Usenix security (Vol. 7, pp. 1-16).

Gu, G., Yegneswaran, V., Porras, P., Stoll, J., & Lee, W. (2009). Active botnet probing to identify obscure command and control channels. In: Computer security applications conference, 2009. ACSAC'09. (pp. 241-253).

Hutchinson, W. and Warren, M. (2001). Principles of Information Warfare. Journal of Information Warfare, 1(1), pp. 1-6.

Libicki, M. (1995). What is Information Warfare? Strategic Forum Number 28, Available at: http://www.dodccrp.org/files/Libicki_What_Is.pdf

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009). Botnet: classification, attacks, detection, tracing, and preventive measures. In: Eurasip journal on wireless communications and networking (Vol. 2009, pp. 1184-1187).

Shanthi, K., & Seenivasan, D. (2015). Detection of botnet by analyzing network traffic ow characteristics using open source tools. In: IEEE 9th international conference on Intelligent systems and control, ISCO 2015 (pp. 1-5).

Stinson, E., & Mitchell, J. C. (2007). Characterizing bots remote control behavior. In International conference on detection of intrusions and malware, and vulnerability assessment (pp. 89-108).

Woodiss-Field, A., Johnstone, M., (2018). Towards a Method for Detecting Botnet Code on IoT Devices. Proceedings of the 2018 Cyber Forensic & Security International Conference, pp. 30-34, Nuku’alofa, Kingdom of Tonga, Christ's University in Pacific.

Zeidanloo, H. R., Shooshtari, M. J. Z., Amoli, P. V., Safari, M., & Zamani, M. (2010). A taxonomy of botnet detection techniques. In: Computer science and information technology (ICCSIT), 2010 3rd IEEE international conference on (Vol. 2, pp. 158-162).

Government Cloud Computing Security Guidelines: Similarities, Differences, and Gaps Related to Cyber Warfare

Mansoor Al-Gharibi, Matthew Warren and William Yeoh
Deakin University Centre for Cyber Security Research and Innovation,
Deakin University, Geelong, Victoria, Australia.
malghari@deakin.edu.au, matthew.warren@deakin.edu.au,
william.yeoh@deakin.edu.au

Abstract: The purpose of this paper is to explore and discuss similarities, differences, and gaps in government cloud computing security guidelines, as they relate to potential cyber warfare. It presents several implementation approaches used by governments, and compares three sets of cloud security guidelines. The data used in the paper were gathered from various academic, governmental and online sources. It was found that although the guidelines varied in terms of detail, none of them addresses the potential for cyber warfare and possible consequences for government cloud security.

Keyword: Cloud Computing, Cloud Computing Security, Cloud Computing Security Guidelines, Cyber Warfare.

Introduction:

Cloud computing is an information technology model whereby computer system resources are made available to the user via the internet, thus reducing or eliminating reliance on the traditional IT delivery model. Cloud computing can be established as a public, private, hybrid, or community cloud. In the public sector, many governments have developed what is termed a “Government Cloud” (G-Cloud) to reduce or eliminate reliance on external cloud service providers.

The implementation of cloud systems aids both productivity and efficiency, and reduces costs through the provision of on-demand services. Additionally, adoption of cloud computing shifts responsibility of IT management to cloud service providers, allowing organisations to focus on core business activities. Additionally, cloud computing is flexible and can be scaled according to business need.

Studies have demonstrated that the public sector can realise a 50% to 67% cost saving by adopting a public or private cloud system (Alford & Morton 2009). Although there exist potential security risks and other considerations, the public sector is swiftly adopting and implementing cloud computing among their IT strategies. In order to manage cloud security risk, many governments have developed cloud security guidelines to assist in protecting the confidentiality, integrity and availability of adopters’ and implementers’ data.

Literature review:

Cloud Computing:

Cloud computing is defined by experts based on key characteristics (Madhavaiah, Bashir & Shafi 2012). It was defined by the National Institute of Standards and Technology (NIST) as, “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance 2011).

Cloud Computing Characteristics:

The key characteristics that differentiate cloud computing from traditional IT modes are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Mell & Grance 2011). While Hurwitz and colleagues (cited in Madhavaiah, Bashir & Shafi 2012) identified elasticity and scalability, self-service provisioning, standardised application program interfaces (APIs), billing and metering of services, performance monitoring and measuring, and security as the key characteristics of cloud computing.

Cloud Computing Service Types:

There are three primary cloud computing services types. These are: infrastructure as a service (IaaS); platform as a service (PaaS); and software as a service (SaaS) (Nirenjena et al. 2017). Each provides a different set of services to cater for the needs of a different type of user, for example, SaaS includes enterprise resource planning (ERP) software, PaaS includes database platforms, and IaaS includes servers' usage.

Cloud Computing Deployment Models

There are four deployment models for cloud computing services. These are termed the public, private, hybrid or community cloud (Mell & Grance 2011; Senarathna et al. 2016). The titles of these deployment models refer to the users of the cloud services infrastructure or a dedicated part of it. For example, in a private cloud setup, resources are dedicated to a single customer, while a public cloud setup resources are shared amongst numerous unassociated customers.

Government Cloud Computing Adoption Approaches

Adoption of cloud computing by governments carries an associated risk to critical infrastructure. Critical infrastructure, according to Pye and Warren (2007), is defined as, "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded, or rendered unavailable for an extended period, would significantly impact upon the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security". Despite the existing risks, governments have nonetheless widely adopted cloud computing systems, using three different approaches (summarised in Figure 1).

In Australia, the Federal government currently employs the Microsoft cloud service "Azure", which operates via data centres located in Canberra, Sydney and Melbourne (Microsoft 2018). France was in favour of developing a nation-wide government cloud, termed "Andromeda," and contracted two companies, Orange and Thales, to undertake this project (Zwattendorfer et al. 2013). In the USA, government entities are acquiring commercial cloud services as per their needs and selection processes. The UK has established its government cloud and has its own software-as-service repository, termed CloudStore, which offers infrastructure, software, platform and specialised services (Zwattendorfer et al. 2013). The Omani government established cloud infrastructure, "G-Cloud", offering IaaS, PaaS, SaaS and business processes as services (Information Technology Authority 2018).

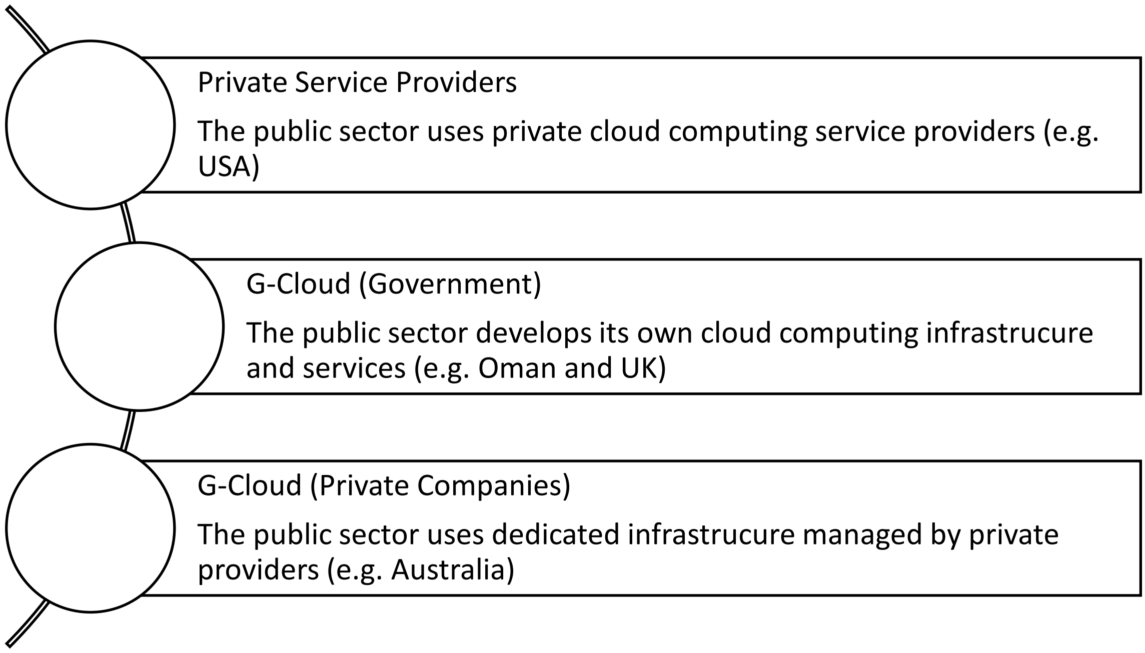

Private Service Providers
The public sector uses private cloud computing service providers (e.g. USA)
G-Cloud (Government)
The public sector develops its own cloud computing infrastrucure and services (e.g. Oman and UK)
G-Cloud (Private Companies)
The public sector uses dedicated infrastrucure managed by private providers (e.g. Australia)

Figure 1: Government Cloud Computing Adoption Approaches

Exploration of Three Governments Security Guidelines

Cloud security guidelines are generally formulated to help protect the data and its confidentiality, integrity and availability (Australian Government 2019a, 2019b; Federal Office of Information Security 2017; U.S. Department of Homeland Security 2018).

Cloud Security Guidelines in Australia

In Australia, there are two guidelines which target the organisations receiving services in addition to the service providers (Australian Government 2019b). These are called “Cloud Computing Security for Tenants,” and “Cloud Computing Security for Cloud Service Providers”. These guidelines discuss cloud computing risks and risk mitigation strategies. They target the cybersecurity team, in addition to cloud architects and business representatives, with a focus on sensitive and highly sensitive data. The guidelines identified 18 risks. They provide 17 mitigations for general risks related to all cloud services types. Also, mitigations for each of the individual service types, including five for IaaS, four for PaaS, and two for SaaS.

Cloud Security Guidelines in America

In the United States, a single set of detailed guidelines, termed “Cloud Security Guidance” targets the federal agencies which plan to use, or are currently using, existing commercial cloud services (U.S. Department of Homeland Security 2018). It identified 30 related considerations and provided templates that address the cloud service model, risk analysis, considerations to guide recommendations, cloud guidance, applicable FedRAMP (The Federal Risk and Authorization Management Program) guidance and controls, and supporting data. Additionally, the guidelines include three use cases by federal agencies already leveraging commercial clouds or in the process of transition. In contrast with the other guidelines examined in this paper, US guidelines have specifically addressed the potential for service outages due to natural causes.

Cloud Security Guidelines in Germany

In Germany, the guidelines are called “Secure Use of Cloud Services” and target persons responsible and employees in cloud usage project groups, IT security officers, responsible IT persons, and decision-makers (management) (Federal Office of Information Security 2017). The guidelines are to aid the target audience to use cloud computing securely. They identify 18 threats, divided into: threats for cloud infrastructure and services; threats when using cloud services; and threats when introducing and using the cloud. The guidelines approach cloud security using project management methodologies, and feature a section addressing risk assessment.

Similarities, Differences and Cyber Warfare Related Gaps

This paper examined Australian, American and German cloud security guidelines. While the Australian and German guidelines targeted specific groups of people in the adopters' entities, the American guidelines target federal agencies more generally. All of the three sets of guidelines address the three cloud service models, IaaS, PaaS, and SaaS. Only the German guidelines did not focus on a specific cloud deployment model. The Australian guidelines focus on public community, and to lesser extent, hybrid and outsourced private cloud, while the American guidelines focus on commercial public cloud.

The Australian and German guidelines are brief and identify eighteen risks, with German guidelines adopting a project management perspective, and Australian guidelines focusing on potential mitigation strategies. The American guidelines, in contrast, offer considerably greater detail, identifying 30 considerations with templates comprehensively analysing each consideration. While only the American guideline addressed service outages due to natural causes, none have specifically examined the risks that can be caused by cyber warfare. Table 1 presents a brief summary of the key guidelines.

Table 1: Comparison between cloud security guidelines in Australia, the United States and Germany

Country	***Document Purpose***	***Target Groups***	***Cloud Service Model***	***Deployment Model***	***Focus of Document***	***Risks/ Considerations***	***Mitigations***
Australia	Designed to assist the target audience to jointly perform risks assessment and use cloud services securely	Cybersecurity team, cloud architects and business representatives	IaaS PaaS SaaS	Public community and to a lesser extent, hybrid or outsourced private	Use of cloud services for sensitive and highly sensitive data and assist in mitigating risk of availability and integrity for non-sensitive data	18	30
United States	To help agencies understand and address risks and challenges to use the commercial cloud environment for their data and applications securely	Federal agencies	SaaS PaaS IaaS	Public commercial Cloud	-	30	Detailed analysis and guidance for each consideration /risk
Germany	To aid the target audience to use cloud computing securely	Persons responsible and employees in cloud usage project groups, IT security officers, responsible IT persons, decision-makers (management)	IaaS PaaS SaaS	Private cloud, community cloud, public cloud, hybrid cloud	Normal and high protection requirements	18	Project managing the cloud service starting with cloud strategy and ending with termination of cloud usage.

Conclusion, Future Research and Recommendations

Cloud computing is an information technology model where IT services are provided as virtual services and can be deployed as public, private, hybrid or community cloud. Cloud services include three service types: infrastructure as service; platform as service; and software as service. There are many advantages to cloud computing, including cost reduction, as well as improving efficiency and security.

Despite potential security risks, many governments have chosen to adopt cloud computing using different implementation approaches. These involve commercial cloud services, government cloud services developed by government, and government cloud services developed by private companies. In order to facilitate secure use of cloud services, cloud security guidelines have been developed, which vary markedly between governments.

The security guidelines presented in this paper have a similar scope and cloud service deployment model coverage, and a similar focus but with different structure and detail levels. The security guidelines examined in this paper have both a similar scope, and coverage of service deployment models, they differ in structure and the level of detail offered. The guidelines studied in this paper did address the risks associated with cyber warfare.

Cloud computing is being adopted and implemented by many governments and by identifying the gaps in the current security guidelines, this paper highlights the need to consider cyber warfare as a risk to be mitigated. This paper also raised the issue of the brief nature of some of the guidelines. Therefore, great need exists to further develop the breadth and depth of these guidelines, addressing various probable risk scenarios and offering potential mitigations.

References

Alford, T & Morton, G 2009, 'The Economics of cloud computing', *Booz Allen Hamilton*.

Australian Government 2019a, *Cloud Computing Security for Cloud Service Providers*, <https://www.cyber.gov.au/node/89>.

Australian Government 2019b, *Cloud Computing Security for Tenants*, <https://www.cyber.gov.au/publications/cloud-computing-security-for-tenants>.

Federal Office of Information Security 2017, *Secure use of cloud services*, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/SecureUseOfCloudServices/SecureUseOfCloudServices.pdf>.

Information Technology Authority 2018, *Oman G-Cloud*, Information Technology Authority, retrieved 05 February 2018, <https://www.ita.gov.om/G-Cloud/G-Cloud.aspx>.

Madhavaiah, C, Bashir, I & Shafi, SI 2012, 'Defining Cloud Computing in Business Perspective: A Review of Research', *Vision (09722629)*, vol. 16, no. 3, pp. 163-73.

Mell, P & Grance, T 2011, 'The NIST definition of cloud computing'.

Microsoft 2018, *Microsoft First to Offer Azure Cloud Regions for Australian Government - Microsoft News Centre Australia*2018, <https://news.microsoft.com/en-au/features/microsoft-first-offer-azure-cloud-regions-australian-government/>.

Nirenjena, S, Divya, A, Aswini, R, Jayalakshmi, S & Saradhambal, G 2017, 'A cloud computing revolution in business perspective', *Advances in Natural and Applied Sciences*, vol. 11, p. 558+.

Pye, G & Warren, M 2007, 'Modelling critical infrastructure systems', *Journal of information warfare*, vol. 6, no. 1, pp. 41-53.

Senarathna, I, Yeoh, W, Warren, M & Salzman, S 2016, 'Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs', *Australasian Journal of Information Systems*, vol. 20, p. 20p.

U.S. Department of Homeland Security 2018, *Cloud Security Guidance*, <https://www.us-cert.gov/sites/default/files/publications/Cloud_Security_Guidance-.gov_Cloud_Security_Baseline.pdf>.

Zwattendorfer, B, Stranacher, K, Tauber, A & Reichstädter, P 2013, 'Cloud Computing in E-Government across Europe', in Berlin, Heidelberg, pp. 181-95.

Fact and Fiction in Technology-Driven Military Decision-Making: Evidence from the US and Israel

Shiri Krebs

Senior Lecturer and HDR Director, Deakin Law School Fellow, Stanford Center on International Security and Cooperation, USA.
s.krebs@deakin.edu.au; shirik@stanford.edu

Abstract

Security decision-making processes have been increasingly relying on technology-generated information, including automated algorithms, big data analytics, and drone imaging. While incorporating valuable information into security decision-making processes, these methods also entail several inherent weaknesses, which lead to erroneous, irreversible, decisions. This article focuses on the role played by technology-generated data in security decision-making processes, and the dangers associated with this heavy reliance on technology. To provide fresh insight into these processes, the article employs interdisciplinary theories of risk assessment, organizational decision-making, and international law, and compares four incidents in which both U.S. and Israeli militaries blamed the technology and its implementation for erroneous targeting of civilians. The article finds that despite their objective and neutral pretence, big data analytics and drone imaging involve value-infused predictions and interpretations which increase the risk of error, while producing a sense of robustness and clarity. Additionally, while these methods increase the volume of available information, they place further challenges on the decision-makers and skew their risk assessment. Instead, it is recommended to redefine “data” for the purposes of security decision-making, to avoid transforming inconclusive information into brute facts, and to mandate further investigation, where needed, rather than completing the missing information with automated processes. Importantly, the outputs of automated communication and intelligence gathering systems should be questioned and re-evaluated to make sure individuals are not being killed based on misrepresentation of the intelligence, and uncritical assessment of the data accuracy and robustness.

KEYWORDS

Big data, automated algorithms, drome imaging, intelligence, fact-finding, heuristics and biases, risk assessment.

Discussion notes:

On October 3, 2015, at 2:08 a.m., a United States Special Operations AC-130 gunship attacked a Doctors Without Borders hospital in Kunduz, Afghanistan, with heavy fire. Forty- two people were killed, mostly patients and hospital staff members. A U.S. military investigation concluded that the attack resulted from several factors, including significant failures of the electronic communications equipment that prevented an update on the fly.

On the morning of February 21, 2010, an OH-58D Kiowa helicopter fired Hellfire missiles and rockets on three vehicles in Uruzgan Province in Afghanistan, destroying the vehicles and killing 23 civilians. A U.S. military investigation report found that inaccurate and unprofessional reporting by the predator drone operators led to the airstrike.[1]

On January 5, 2009, around 6:30 a.m., Israeli forces fired several projectiles at the Al-Samouni family house south of Gaza city, killing twenty-one family members who took refuge in that house.[2] An Israeli military investigation found that this attack resulted from erroneous reading of a drone image.[3]

On July 22, 2002, the Israeli Air Force dropped a one-ton bomb on Hamas' operative Salah Shehadeh's house in Gaza City, killing, in addition to Shehadeh and his assistant, 13 civilians, 8 of them children.[4] An Israeli commission of inquiry found that the heavy and unintentional collateral damage resulted from erroneous assessments of the available intelligence, including misinterpretation of aerial images.

These four examples represent cases in which U.S. and Israeli armed forces acknowledged operational errors that led to mistaken attacks on civilians. The unintentional killing of civilians in each of these examples was attributed by both U.S. and Israeli militaries to errors relating to electronic systems, technology-generated data, and the way in which the data were utilized by military personnel and processes. These, and many other, similar, incidents demonstrate an urgent need to reconsider the heavy reliance on technology during

[1] *AR 15-6 Investigation, 21 February 2010. Air-to-Ground Engagement in the Vicinity of Shahidi Hassas, Uruzgan District, Afghanistan*, HEADQUARTERS UNITED STATES FORCES, AFGHANISTAN, 21 May 2010. Available at: https://archive.org/details/dod_centcom_drone_uruzgan_foia/page/n1

[2] The Goldstone Report, *supra* note 5, at 161-62.

[3] ISR. MINISTRY OF FOREIGN AFFAIRS, GAZA OPERATION INVESTIGATIONS: SECOND UPDATE 6 (2010), http://www.mfa.gov.il/mfa/foreignpolicy/terrorism/pages/gaza_operation_investigations_second_update_ju ly_2010.aspx; Amira Hass, *What Led to IDF Bombing House Full of Civilians During Gaza War?*, HAARETZ (Oct. 24, 2010), http://www.haaretz.com/israel-news/what-led-to-idf-bombing-house-full-of-civilians-during-gaza- war-1.320816 [https://perma.cc/Y65P-HXM2] (archived Dec. 31, 2017). .

[4] Meyerstein, '*Case Study*'.

real-time military decision-making, and to identify effective methods to better incorporate technology-generated data in military decision-making processes, alleviating some of its inherent weaknesses.

A growing literature has been identifying the growing reliance on technology- generated data in military decision-making, including big data analytics, automated algorithms, and drone imaging.[5] As their level of autonomy and sophistication increases, these technologies are becoming an inseparable part of military decision-making, and their utilization is constantly increasing. The general notion is that these new technological developments improve decision-making processes by providing immediate, accurate, relevant, and timely information that complements traditional forms of information-gathering and assists decision-makers in reaching more accurate decisions.[6] However, as this article argues, while adding valuable information, these methods place additional burdens on decision- makers, and may hinder the decision-making process rather than improve it. In particular, it is argued that reliance on big data analytics and real-time drone imaging *masks the human factor and the potential of error*, by presenting the outputs as objective, complete, and neutral; and that it *disguises value-judgements and predictions as brute facts*, triggering organizational biases and mistaken interpretation and implementation of the data. The heavy reliance on sophisticated predictive technology, combined with preventive legal regimes, engenders *law- fulfilling prophecies* which are prone to erroneous risk assessments and produce data-generated avatars that replace the real persons – or the actual conditions on the ground – with no effective way available to refute these virtual representations. The result is faulty decision- making processes that are continuously leading to irreversible, deadly, outcomes.

This paper employs interdisciplinary theories of risk assessment and organizational decision-making to analyse the new fact-finding techniques which have been increasingly utilized during military decision-making processes. The paper deals specifically with the new challenges arising from the reliance on big data analytics and drone imaging in two

[5] See, among others, Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, 163 U. Pa. L. Rev. 327; Johnson, Benjamin, "Second Prize: Coded Conflict: Algorithmic and Drone Warfare in US Security Strategy." *Journal of Military and Strategic Studies* 18, no. 4 (2018); Suchman, Lucy, Karolina Follis, and Jutta Weber. "Tracking and Targeting: Sociotechnologies of (In) security." (2017): 983-1002; Weber, Jutta. "Keep adding. On kill lists, drone warfare and the politics of databases." *Environment and Planning D: Society and Space* 34, no. 1 (2016): 107-125; Oron-Gilad T, Parmet Y. Close target reconnaissance: a field evaluation of dismounted soldiers utilizing video feed from an unmanned ground vehicle in patrol missions. Journal of Cognitive Engineering and Decision Making. 2017 Mar;11(1):63-80.
[6] Barnes, M., & Jentsch, F. (Eds.). (2010). Human-robot interactions in future military operations, Burlington, VT: Ashgate; Ntuen, C. A., Park, E. H., & Gwang-Myung, K. (2010). Designing an information visualization tool for sensemaking. International Journal of Human–Computer Interaction, 26(2–3), 189–205

jurisdictions: the United States and Israel, by shedding light and learning from a careful analysis of the four erroneous attacks described above. These four cases were selected because they represent a variety of technology-related operational failures, as well as due to the rarity in which detailed military findings concerning operational failures are provided to the public.

Mark Twain, quoting Benjamin D'israeli, stated in his autobiography already in 1904 that there are three types of lies in the world: lies, damn lies, and statistics.[7] The point was, that statistical calculations and predictions are misleading, deceiving, and biased.[8] Indeed, statistical calculations and predictions, which today are often produced using big data analytics and complex algorithms, have very different qualities than brute facts. The data can be presented in different ways, analysed using different methods, and can tolerate different interpretations.

To improve the outcomes of military decision-making, this article recommends, based on lessons learned from the four case studies, several means to better incorporate technology- generated data into military decision-making processes. First, greater transparency is required concerning the completeness, certainty, and reliability of the relevant data, the way it was generated, and its limitations. Second, value-judgments and predictions should be highlighted and separated from brute facts. Third, drone imaging and its interpretation should be compared with and completed by other sources of information. Fourth, where information is missing, it should not be completed by algorithms and assumptions, but rather may warrant further investigation and collection of additional information. Finally, the outputs of drone imaging and automated algorithms should be questioned and re-evaluated, making sure individuals are not being killed based on misrepresentation of the data, and uncritical evaluation its accuracy and robustness. Technology-generated data has many promises for military decision-making; at the same time, it can trigger erroneous decision- making processes leading to the loss of human lives. At a time when preventive legal regimes are increasingly aligned with predictive fact-finding processes, it is essential to develop effective ways to better integrate predictive technology-generated data into decision-making processes based on lessons learned from many war room failures.

[7] Mark Twain, *Autobiography*, Volume I (Berkeley, Los Angeles and London: University of California Press, 2010), p. 228. This quite, however, was probably wrongly attributed to D'Israeli, and it is uncertain who was the first to coin it. See: Lies, Damn Lies, and Statistics, Department of Mathematics, University of York (2012), available at: https://www.york.ac.uk/depts/maths/histstat/lies.htm.

[8] Mark Twain, *Autobiography*, at 228.

Information Warfare by Proxy: Malware in PLC Firmware

Lachlan Walling, Michael N. Johnstone and Peter Hannay
School of Science
Security Research Institute
Edith Cowan University
Western Australia
lwalling01@our.ecu.edu.au, {m.johnstone, p.hannay}@ecu.edu.au

Abstract: *Attacks on Industrial Control Systems (ICSs) can lead to plant shutdown and destruction of property that can cost millions in damages and lost production. Even worse, such attacks can result in loss of life, for example, if malware placed on devices were to cause equipment to explode and/or release toxic fumes. More serious could be attacks on critical infrastructure, where as well as damage and loss of life at a plant, many people could be left without services such as water, gas or electricity. In addition, the output of industrial systems can be vital to a country's economy. Due to the potential damage that could be caused by such risks being realised, more research into the feasibility of firmware attacks and how to detect them is needed. We observe some problematic aspects of detection of tampering in software. Our contribution is to examine challenges in ICS security with respect to embedded firmware and to suggest mitigations.*

INTRODUCTION

Industrial control systems (ICSs) are systems used for monitoring and automating operations in critical infrastructure such as water, electricity and transportation. There are many types of control systems such as supervisory control and data acquisition (SCADA) and distributed control systems (DCS). Specialised devices used in ICSs include programmable logic controllers (PLCs) and remote terminal units (RTUs). PLCs interface with the hardware, taking input from sensors (e.g., switches or level sensors) and controlling actuators (e.g., pumps, motors or alarms) in response. Remote terminal units are devices which monitor sensors and send telemetry back to supervisory systems which display the plant status in a graphical interface for human operators (Babu, Ijyas and Varghese, 2017).

There is growing concern over the security of supply chains across ICS environments (Greene & Johnstone, 2018; Hawk & Kaushiva, 2014). The United States Government is also concerned about supply chain attacks after the compromise of military contractors (Nissen, 2019). Devices need to be produced by a manufacturer using parts produced by other manufacturers and sent to the customer. The manufacturers and the client may be in different countries. This gives an attacker multiple places to intercept and tamper with the device or parts of it. This also applies to software. Device firmware, when updating is allowed, is commonly verified using digital signatures or hashing. This allows the customer to check whether their firmware image matches one produced by the manufacturer that is presumed to be secure. This prevents tampering between the manufacturer and the customer. However, if the manufacturer is compromised the firmware image that the signature is computed on may be modified to contain malicious code (Basnight, Butts, Lopez, & Dube, 2013a). In this case it would be beneficial to have a method of determining the security of the firmware based on its contents, which determines its actual behaviour.

In the following section we examine the difficulty of detecting changes in PLC firmware, especially when it is compromised at the source.

Detection of Tampering in Firmware

Injecting malicious code into PLC firmware is extremely difficult to detect since such code may be injected in a supply chain compromise between the manufacturer and customer instead of breaching a customer's network.

The main methods of detecting firmware tampering are hashing and/or digital signatures to verify the firmware before uploading it to the device. However, it is not impossible for malicious firmware to be signed by the manufactures private key if the key has been compromised (Basnight, Butts, Lopez, & Dube, 2013b). For example, Stuxnet was signed using trusted certificates (Dunn, 2019), and more recently, ASUS's updater was hacked to send out a malicious signed update (ASUS, 2019). A PLC manufacturer's download site could potentially also be hacked to provide a maliciously-modified firmware. Reverse-engineering and examining the firmware to see how it actually behaves is possibly the only way of knowing whether the firmware can be trusted.

Some methods have been researched in order to detect malicious changes to control logic and firmware. Research has been undertaken in creating devices to intercept control logic downloaded onto PLCs to help an engineer determine if it will behave as expected even if a workstation has been compromised. Yang et al. (2018) suggest adding runtime behaviour monitoring to PLC firmware which compares the values being written by the PLC and the timing with a specification for some of its behaviour, such as valid output ranges. Davidson, Davidson, Moench, Ristenpart, and Jha (2013) used symbolic execution to find vulnerabilities in firmware for MSP430 microcontrollers, but their tool requires source code.

Some methods have been researched in order to detect malicious changes to control logic and firmware. While there is some public research on detecting vulnerabilities in firmware, there seems to be a lack of research specific to PLCs.

Further, generic research on detecting malware and vulnerabilities in firmware may not be directly applicable to PLCs for several reasons. Firmware intended for more general-purpose devices such as phones is often a general-purpose operating system (such as the Linux kernel in the case of Android) with application software for the user interface and drivers specific to the hardware. This is in contrast to PLCs which tend to have monolithic firmware; instead of a general-purpose kernel with a file system and application software, the firmware is a single binary program of just a kernel. In addition, common strategies of malware detection such as signature scanning may not be as applicable to PLCs. Table 1 lists key challenges in maintaining the security of PLCs and some potential mitigations.

Table 1: Challenges in PLC security and their mitigations

Challenge	Mitigation(s)
Insecure network protocols, e.g. replay attacks, pass the hash	Using more secure protocols; Isolating access to the subnet through a VPN
Modifying the control program	Good security practices that help stop an attacker from being in the position of modifying the program (e.g., by compromising a workstation); Bump in the wire devices that allow an engineer to verify the behaviour of the transmitted program. Can also potentially use logical methods to automatically verify against security constraints; Monitoring, in firmware or external
Attackers modifying the firmware	External monitoring; Signing, though keys may be compromised; Reverse engineering to find malware – Need to understand the structure of the firmware – Need to locate the malware in the firmware
Attackers exploiting the firmware	Fuzzing – Embedded devices tend to hang or continue in an incorrect state instead of an observable crash; Reverse engineering to review code

	– Need to understand the structure of the firmware – Need to find vulnerabilities

Conclusion

Whilst there are no published examples of malware in PLC firmware, the threat is a subtle one and should not be dismissed. Given the plethora of suppliers of SCADA-based systems (each with their own code base), the threat surface is large and complex. The shift from the deployment of PLCs to RTUs, may in some part, reduce the potential for threats to be realised, but the rapid development of the Industrial Internet of Things (IIoT) and large deployments of IIoT devices may negate any security gains. Current approaches to integrity checking in software management and delivery systems, such as code signing or hashing would not detect a threat where malware was injected at the source (because the source is inherently trusted by the deployment). Static approaches such as reverse engineering show promise but are constrained by time-they are labour-intensive, even with sophisticated tool support. Dynamic approaches are problematic in an ICS space as plant availability or production is valued over any other security-related driver. Clearly, more work needs to be done in this area, given the significant economic loss that would be caused by a failure of critical infrastructure-perhaps machine learning systems could assist given the volume of data.

References

ASUS. (2019). Asus response to the recent media reports regarding asus live update tool attack by advanced persistent threat (apt) groups. Available at https://www.asus.com/News/hqfgVUyZ6uyAyJe1.

Babu, B., Ijyas, T., & Varghese, J. (2017). Security issues in SCADA-based industrial control systems. In 2017 2nd international conference on anti-cyber crimes (ICACC) (pp. 47–51). doi:10.1109/Anti-Cybercrime.2017.7905261

Basnight, Z., Butts, J., Lopez, J., & Dube, T. (2013a). Analysis of programmable logic controller firmware for threat assessment and forensic investigation. Journal of Information Warfare, 12(2), 1–9, IV.

Basnight, Z., Butts, J., Lopez, J., & Dube, T. (2013b). Firmware modification attacks on programmable logic controllers. International Journal of Critical Infrastructure Protection, 6(2), 76–84. doi:10.1016/j.ijcip.2013.04.004

Davidson, D., Moench, B., Ristenpart, T., & Jha, S. (2013). Fie on firmware: Finding vulnerabilities in embedded systems using symbolic execution. In: 22nd Usenix security symposium (usenix security 13) (pp. 463–478).

Dunn, S. (2019). The scary and terrible code signing problem you don’t know you have. Retrieved from https://www.sans.org/reading-room/whitepapers/critical/scaryterrible-code-signing-problem-you-36382

Greene, R. and Johnstone, M. (2018). Secure smart contract supply chains. In Proc.17th Australian Cyber Warfare Conference (CWAR) (pp. 6–17). Melbourne, Victoria, Deakin University Centre for Cyber Security Research.

Hawk, C. and Kaushiva, A. (2014). Cybersecurity and the smarter grid. The Electricity Journal, 27(8), 84–95. doi:https://doi.org/10.1016/j.tej.2014.08.008

Nissen, C. (2019). Supply chains may pose weakest security link. Retrieved from https://www.afcea.org/content/supply-chains-may-pose-weakest-security-link

Yang, H., Cheng, L., & Chuah, M. C. (2018). Detecting payload attacks on programmable logic controllers (PLCs). In: 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1–9). doi:10.1109/CNS.2018.8433146

Cyber Secure Geelong: Determining SME Cyber-Security Preparedness

Graeme Pye graeme.pye@deakin.edu.au Deakin University Geelong
Scott Salzman scott.salzman@deakin.edu.au Deakin University Warrnambool
Matthew Warren matthew.warren@deakin.edu.au Deakin University Burwood
Damien Manual damien.manual@deakin.edu.au Deakin University Burwood
Bernadette Uzelac bernadette.uzelac@geelongchamber.com.au Geelong Chamber of Commerce

Keywords: Cyber-Security, SME, Preparedness, Awareness.

Abstract

The Centre for Cyber Security, Research & Innovation (CSRI)* research group at Deakin University in partnership with the Geelong Chamber of Commerce (GCoC) undertook an online cyber-security survey involving the GCoC business membership community. The intention of this research project is to seek and report upon the attitudinal feedback of Small to Medium Enterprise (SME) businesses to measure their cyber-security preparedness, engagement, awareness, resilience and identify potential cyber-security gaps within the broader business community.

Introduction

The GCoC is a business association consisting of nine hundred (900) member organisations. Ninety-five percent (95%) of members are categorised as SME businesses with less than twenty (20) employees. Furthermore, there is a diverse number of differing business categories within the GCoC membership cohort and each business will have their own contextual interpretations of their cyber-security posture and information management capabilities (GCoC, 2019).

While technology has enabled more individuals and businesses alike to connect to the Internet, it has also enabled criminals to exploit new victims as demonstrated with 13, 500 incidents of cybercrime reported in the past three months to the Australian Cyber Security Centre (ACSC). Resulting in lost money via online fraud, identity fraud and ransomware attacks with email compromise being the most prevalent social engineering cyber-security issue for businesses. The per annum cost of cyber-security incidents to Australian business is estimated to be up to $29 million (Borys, 2019).

Business cyber-security experiences may be similar or differ significantly based on resources, individual and business capabilities and investment in managing cyber-security and information management practices, regulation, policies, training commitment and cultural awareness. This case study serves as a pilot online survey for a broader Australia-wide research related survey.

Geelong Case Study:

Geelong is the second largest port city in regional Victoria, Australia and is situated on the shores of Corio Bay approximately 75km south-west of the state capital Melbourne. The business opportunities have diversified from a traditionally narrow largely heavy manufacturing capability and associated businesses. Towards a more broader innovative and diverse industry base including emerging health care, education research and training, retail, agriculture and advanced manufacturing (Geelong Australia, 2018).

Research Questions

Analysis of cyber-security broadly identifies that the presence of the following three (3) key elements indicates the existence of a cyber-secure environment, 1. Confidentiality, 2. Integrity and 3. Availability of the respective business information systems. If any or all of these elements are not evident, then the cyber-security environment is considered as insecure.

Research Question 1: Are there any significant differences or similarities in the way GCoC members manage their cyber-security status?

Research Question 2: What are the identifiable cyber-security issues and gaps relating to the way GCoC members secure their business environment?

Research Question 3: What are the identifiable cyber-security factors, policies, levels of awareness and cultural issues that impact GCoC members?

If any differences, similarities, inconsistency or lack of cyber-security presence findings are identified, what implications could this have on current business cyber-security practices within the Geelong regional business community? What prioritised recommendations should be forthcoming?

Research Method

Geelong area SMEs were invited to participate in an online survey via email invitation seeking responses from within the membership list of the GCoC. All respondents were informed via the survey's Plain Language Statement as to the anonymous nature and intent of the cyber-security survey and that their informed consent will be sought prior to accessing the online survey instrument, which aligns with Deakin University's Research Ethics Policy.

The online survey invitations were sent out via email and consisted of an additional two (2) reminder emails to prompt and illicit responses over a four (4) week period commencing March 2019. The survey questionnaire consisted of a maximum of thirty (30) questions including forced and free-format text question responses. The data was collected using the Qualtrics software package managed by Deakin University and was analysed using Microsoft Excel. Data was extracted from the Qualtrics platform in Microsoft Excel comma delimited format and coded for subsequent analysis. All data was checked to ensure consistency in representation and formatting so that subsequent analysis was possible. As the number of observations was limited (n = 15) and the sample method was self-selection, summary statistics only are provided. While the summary information presented in this research provides valuable insight, it is noted that proportions represented in self-selecting surveys can be misrepresentative.

Online Survey Themes

The following general constructs of the research sought to illicit responses relating to an appreciation and understanding of the current Geelong SME business cyber-security status:

- *SME Demographics* - to illicit general information about particular business demographics
- *Cyber Security Confidence* - to determine the initial confidence of the business's cyber-security strategic setup.
- *Cyber Security Awareness and Culture* - to determine the level of cyber security awareness and culture within the business.
- *Cyber Behaviours and Practices* - to determine workplace behaviours and practices.
- *Cyber Security Policies* - to find out what policies, if any, are established and followed.
- *Cyber Security Measures* - to find out what security measures are in place.
- *Business Continuity Planning* - Business continuity planning describes the processes and procedures a business puts in place to ensure that essential functions can continue during and after an incident, including an immediate incident response and disaster recovery to enable business continuation and recovery.
- *Information Security Management* - to determine information disclosure breaches and information or data management practices.
- *Cyber Security Feedback* - the final part of the survey inviting ad hoc comments and details concerning the business surveyed.

Upon analysis of all the data collected, recommendations and possible solutions will be subsequently provided to assist and guide businesses with best practice approaches designed to address cyber-security gaps and bolster cyber-security within the SME business community. Additional, and specific cyber-security and information management advice will also be offered to those businesses requiring further specific educational, awareness and technical assistance.

Online Survey Response Rate and SME Demographics

Approximately 900 Geelong Chamber of Commerce registered businesses were emailed an invitation and link to participate in the survey. Of these, 15 responded, with 2 of those 15 responses, failing to complete all of the questions on the survey. This represents a response rate of 1.7%

Six, or 40% of the responses, came from the business professional and commercial services industry sector. Five of the responses were from businesses claiming to have traded for more than 20 years. All responding businesses indicated that they use the Internet in some way.

Key Online Survey Analysis Findings

When respondents were initially asked where their business first learnt about cyber-security and a baseline starting point, 40% of respondents indicated that they had no formal training and were self-taught when it came to their business and cyber-security. Other notable initial findings from the online survey participant s responses have revealed some interesting insights as per the following research themes too.

Cyber Security Confidence

Most individual respondents (84.6% or greater) indicated that they felt at least somewhat confident, very confident or extremely confident in managing the perceived cyber-security risks as follows:

- Uncontrolled use of mobile devices including phones, tablets, laptops (92.3%).
- Incorrect system configuration (100%).
- Internet downloads (100%).
- Malware i.e. malicious software (100%)
- Emails viruses (100%).
- Hacking attempts by external hackers (84.6%)
- Insider attacks by disgruntled employees (91.7%).
- Email scams (92.3%).
- Disclosure of business or customer information (92.3%).

These results indicate that in general the individual responding to the online survey felt at least somewhat confident in their ability to manage the listed cyber-security risks if they occurred.

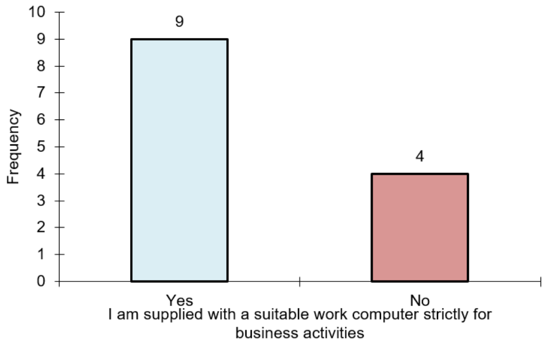
Cyber Security Awareness and Culture

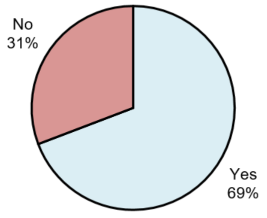
When it came to how important cyber-security awareness of other employees was to the business. Individual respondents mostly (84.6%) indicated that cyber-security awareness was important, with 15.4% of respondents indicating that it was more important than anything else.

Furthermore, when respondents were asked if other employees within the business could recognise a cyber-security incident, 62% of respondents indicated that they could recognise a cyber-security incident. Yet when it came to providing employee training to raise cyber-security awareness, 15% of respondents indicated no training was provided with only a further 15% indicating that only minor training was provided.

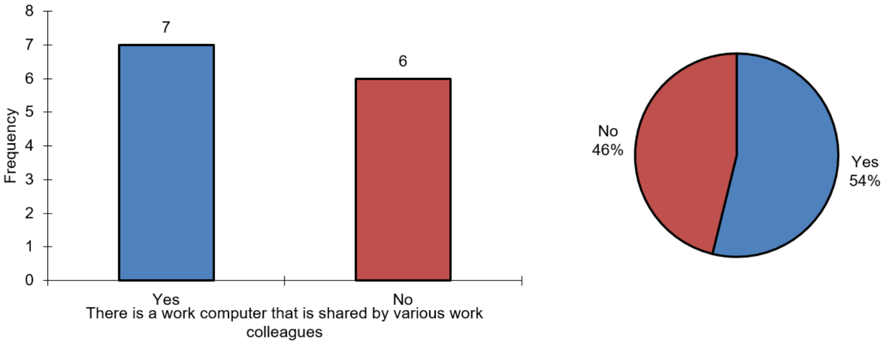
Cyber Behaviours and Practices

Of the listed practices, respondents were able to select multiple "primary uses". The most widely indicated use is for email communication purposes (21% of all claimed uses). The following graphs represent the working behaviours of the respondents.
I am supplied with a suitable work computer strictly for business activities.

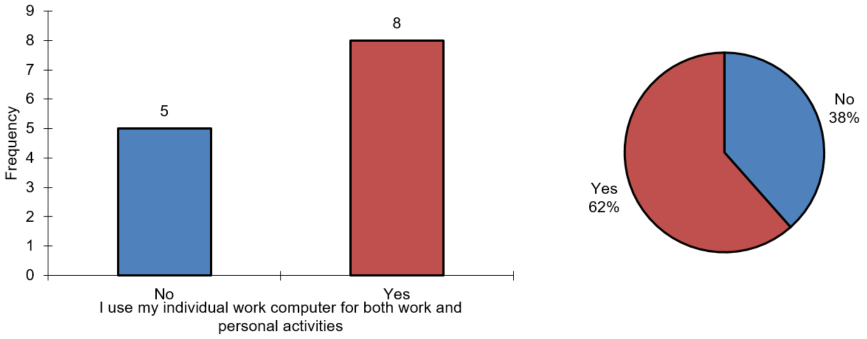




There is a work computer that is shared by various work colleagues

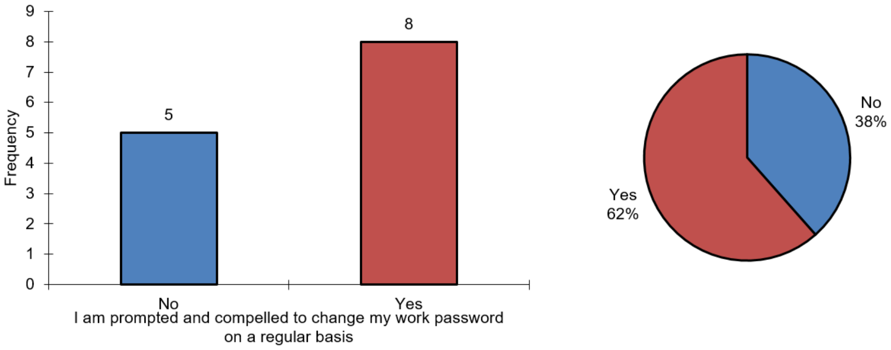


I use my individual work computer for both work and personal activities



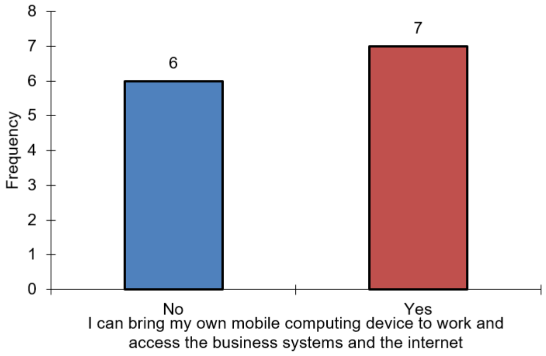
When it came to filtering software, 100% of respondents indicated that they used filtering software to restrict access to harmful Internet sites and when asked whether a specific password is required to access their work computer. 100% of respondents indicate password access is required for work computers.

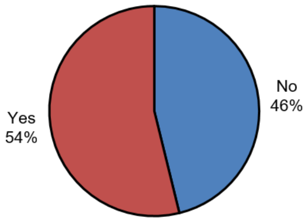
I am prompted and compelled to change my work password on a regular basis



100% of respondents indicated that there is a firewall existing between my work computer and the Internet.

I can bring my own mobile computing device to work and access the business systems and the Internet





Next respondents reported that the top three cyber-security issues over the last two years were as follows:

- Email attacks relating to phishing emails and scams (31%).
- Hacker attacks, externally based (20.69%).
- Virus attacks (17.24%).

This outcome indicates that 31% of the cyber-security issues were a function of email attacks.

When it came to seeking help or action advice most people (41%) would seek assistance from an IT professional.

Cyber Security Policies

Respondents asked if their business had a cyber-security policy. 69% of respondents indicated that they do not have a cyber-security policy. Additionally, 69% of respondents indicated that their business did not have a policy regarding the use of business or employee email. When it came to a BYOD policy, 30.77% indicated that there was indeed a policy in place with a further 38.46% of respondents indicating that they were provided with the necessary mobile devices and had no need for a BYOD policy.

Cyber Security Measures

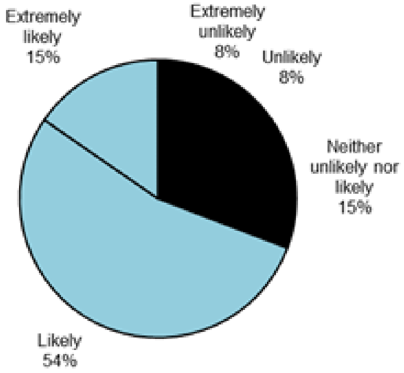
Interestingly, when respondents were asked if they applied or adhered to any IT process or security frameworks and/or security standard. 30.77% of respondents were unsure if this was a business requirement.

Business Continuity Planning

A good outcome was that 69.2% of respondent businesses had a functioning Disaster Recovery Plan (DRP) with a further 61.5% of respondent businesses also having an Incident Response Plan (IRP).

Information Security Management

Respondents were asked how confident they were that their employees possessed the information management knowledge and skills needed to maintain the security of your critical information assets. Notably, 15.38% of respondents were not confident that their employees had the skills necessary to maintain critical information security. Additionally, respondents were asked what would be the likelihood of their business investing in information management awareness and training. As the following graph indicates:



Most respondents (69%) indicate that their business is likely to invest in information management awareness and employee development solutions in an ongoing manner.

Research Question Responses

RQ 1: Are there any significant differences or similarities in the way GCoC members manage their cyber-security status?
Yes there is, by and large businesses are self-taught when it comes to managing cyber-security risks and are confident that they can deal with most cyber-security risks. With a majority of users indicating that they are compelled to change their access password on a regular basis. Many SME's do have active DRP and IRP in place within their SME to protect valuable information.

RQ 2: What are the identifiable cyber-security issues and gaps relating to the way GCoC members secure their business environment?
There is an indication that a large proportion of SME staff are utilising and accessing a single shared common computer system within their business. Along with an indication that many users are using their work computer for both business and personal activities. Furthermore, survey respondents indicated a lower level of confidence in their colleague's skills when it came to dealing with cyber-security issues or managing information security within the business.

RQ 3: What are the identifiable cyber-security factors, policies, levels of awareness and cultural issues that impact GCoC members?

There is an indication that approximately two-thirds of respondents are using their own mobile devices at work without any policy coverage and there is some confusion or misunderstanding of the potential benefit of adhering to a security standard.

Future Research

Additionally, research will be undertaken via additional focus groups. These groups will consist of voluntary participants who have indicated their willingness to participate from within the online survey respondents. The intention of the focus groups is to illicit qualitative feedback about the interactions of business people with cyber-security, associated technologies, policies and awareness within their respective businesses.

Conclusions

The cost of cyber security issues to Australian businesses is well documented. A Microsoft commissioned study for example, reported that the direct costs to Australian businesses each year is $29 billion per year (Microsoft, 2018). Noting that businesses can be threatened, at risk, or under actual attack from cyber-security incidents and not realise, as well as noting that making any public statement about such threats, risks or attacks has the possibility of affecting an organisations public image, including current and prospective investor perception (and therefore effecting investor decisions), the information sought in this type of research is very difficult to obtain. That is, identifying and quantifying the perceived and actual threats to businesses is a monumental task, as is evidenced in this research, with only 1.7% of the Geelong Chamber of Commerce registered businesses responding. Nonetheless, this research provides an important summary information from which, business perspectives of cyber security issues that are important and relevant to their trading landscape, can begin to be considered and recorded.

The cyber-security summaries derived from this research will focus on delivering insightful cyber-security advice to address the identified issues and security gaps within GCoC businesses. With the intent to then assist and support those individual businesses seeking to address and upgrade their own specific cyber-security capabilities, readiness, awareness and information asset management processes.

Lastly, from the perspective of business, this research should enable a business to increase their respective cyber-capabilities, education and resilience by assisting them to identify, reduce and manage their cyber-risks. This research should give rise to improved business outcomes, through balancing informed cyber-security protection and information asset management, with competing business goals.

References

Borys S. (2019) You could soon be a victim of cybercrime — here's how to try to stop that happening https://www.abc.net.au/news/2019-10-07/cyber-crime-how-to-help-protect-yourself/11577930 Accessed October 2019.
GCoC (2019) Geelong Chamber of Commerce Overview https://www.geelongchamber.com.au/about-us/overview-/ Accessed August 2019.
GeelongAustralia (2018) Work and Investment https://www.geelongaustralia.com.au/geelong/article/item/8d4ad9e1505f93c.aspx Accessed August 2019.
Microsoft (2018) Direct costs associated with cybersecurity incidents costs Australian businesses $29 billion per annum https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/ Accessed September 2019.

*Research undertaken as part of **The Centre for Cyber Security, Research & Innovation (CSRI)** cyber-security research centre located at Deakin University. See https://www.deakin.edu.au/csri

Strengthening Indonesia Digital Economy: Issues, Risks and Challenges in E-Commerce Cyber security

Caroline Chan[1,2], Eugene Sebastian[2], Mathew Warren[3],

[1]RMIT University
[2]Australia Indonesia Centre (AIC)
[3]Deakin University

Abstract

The digital economy is important for Indonesia and is projected to grow to US$120 billion by 2020, comprising about 12 per cent of its GDP. Indonesia faces two challenges to its future digital growth and integration into the global digital economy. First, ensuring the integrity of the security of online business transactions and exchanges. Without reliable cybersecurity systems, 150 million Indonesian internet users remain exposed to security threats. Second, tackling the critical shortage of skilled cybersecurity professionals, which is impeding competitiveness and growth. The Indonesian government estimates that its digital industry needs to skill-up 600,000 workers a year to support business IT functions. This paper provides an overview of the key issues, risks, and challenges to Indonesia's growing digital economy. Based on desktop research, it reviews policy and industry reports, academic literature, and online/digital media. The paper identifies opportunities for Indonesia to accelerate the growth of its digital economy through cybersecurity policies and regulatory strengthening and the development of a national skills and training framework.

E-commerce in Indonesia

Indonesia's e-commerce sector comprises US$5 billion of formal e-tailing and more than US$3 billion of informal commerce (Das, Tamhane et al. 2018). Companies like JD, Lazada, Shopee, and Tokopedia are flourishing in the country. New and smaller online retailing start-ups are also proliferating. Indonesia has the largest online commerce market in Southeast Asia, with revenues predicted to grow to $20 billion by 2022.

A significant driver to Indonesia's e-commerce growth is the increasing number of Micro, Small, and Medium Enterprises (MSMEs) participating online. Micro sized enterprises are defined as enterprises that typically generate annual revenue that is less than IDR300M (~ AUD 30,000); small with revenue of between IDR300M and IDR2.5B (~AUD 250,000); and medium with annual revenue of more IDR2.5B. MSMEs account for 99 per cent of all business in Indonesia and provide 89 per cent of private-sector employment in the country (Asia Pacific Foundation of Canada, 2018).
According to consultancy, McKinsey & Company, the number of online sellers in Indonesia had doubled each of the past three years to reach 4.5 million active sellers in 2017. About 99 per cent are micro enterprises selling their own products, resellers or distributors.

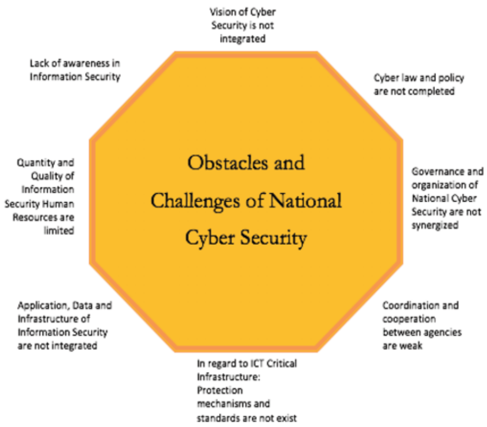
MSME's growth is driven by population size and the rapid expansion of mobile phone users with the highest rate of e-commerce use. Out of a total of 268 million population, 91 per cent of Indonesian adults use any type of mobile phone, while 60 per cent of them are smartphone users. (We are social, 2019). Further, Indonesia boasts the highest rates of e-commerce users of any country in the world, with 90 percent of the country's internet users between the ages of 16 and 64 reporting that they already buy products and services online. (We are social, 2019)

The existence of a robust cybersecurity system is crucial for Indonesia's rapidly expanding digital economy and to fully realise its financial and non-financial benefits - from enterprise growth, international trade, to employment and digital social inclusion.

Indonesia national cyber security

Indonesia's cyber security is starting up. In January 2018, the government established a national cyber security agency, Badan Siber dan Sandi Negara (BSSN) as part of its national critical infrastructure, create standards for industry and support its growth. Currently, Indonesia has no national cyber security strategy in place. International collaboration is a core element in Indonesia's cyber security strategy. In September 2018, Indonesia signed a bilateral Memorandum of Understanding on cyber security cooperation with Australia (Austrade, 2019). Two months later, Indonesia and the United States agreed on a cyber security pact.

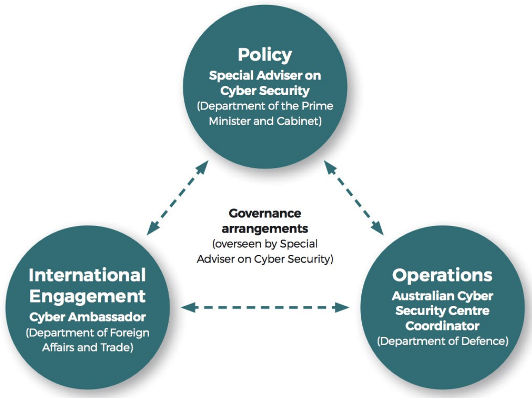
Figure 1 Indonesia National Cyber security – Obstacles and Challenges (Nugraha and Putri 2016)


Vision of Cyber Security is not integrated
Lack of awareness in Information Security
Cyber law and policy are not completed
Obstacles and Challenges of National Cyber Security
Quantity and Quality of Information Security Human Resources are limited
Governance and organization of National Cyber Security are not synergized
Application, Data and Infrastructure of Information Security are not integrated
Coordination and cooperation between agencies are weak
In regard to ICT Critical Infrastructure: Protection mechanisms and standards are not exist

Nugraha and Putri (2016) attempted to map the landscape of cyber security in the country. They identified the various stakeholders and regulations associated with cyber security and found that Indonesia's cyber security is largely focussed on national security and protection of its infrastructure and less on commercial activities, which presumably are viewed as the responsibility of the private sector. Nevertheless, their investigation portrays a complex environment of cyber security in Indonesia, with many obstacles and challenges (See Figure 1) and major issues related to the human factor, governance, and infrastructure.

While Indonesia does not yet have a national cyber security, Australia on the other hand has a comprehensive cyber security strategy it released in 2016. The strategy consists of three pillars policy, operations and international engagement (Figure 2).

Figure 2 Australia Government Security Architecture (Australia Cyber security Strategy 2016 p.24)


Policy
Special Adviser on Cyber Security
(Department of the Prime Minister and Cabinet)
Governance arrangements
(overseen by Special Adviser on Cyber Security)
International Engagement
Cyber Ambassador
(Department of Foreign Affairs and Trade)
Operations
Australian Cyber Security Centre Coordinator
(Department of Defence)

Policy is driven by the Prime Minister office ensuring leadership and advocacy of the work.

Operation is managed through the Australian Cyber Security Centre (ACSC) which guides the nation cyber security priorities. ACSC also provides cyber security advice in the form of Consumer Guides, Australian Communications Security Instructions and other cyber security-related publications; and

The Department of Foreign Affairs and Trade leads Australia's international effort ensuring a coordinated approach to cyber security in the region.

Additionally, ACSC plays significant roles in promoting and improving cyber security awareness to small businesses and consumers, encouraging a safer environment for E commerce activities.

When considering Indonesia's cyber security environment, four key issues stand-out: human capital and capacity development, policies and regulations, digital infrastructure and the global/international environment. Table 1 provides a summary of the issues, risks and challenges in Indonesia cyber security environment.

Table 1: Issues, risks, and challenges in Indonesia's cyber security environment

Issue	Risks	Challenges
Human capital and capacity development	Unable to achieve targets	Digital literacy Lack of awareness of cyber security threats Mismatch between workforce skills and employer/industry skill requirements Lack of skilled cyber security workforce Skills and competencies curriculum do not meet global standards (e.g. CSEC2017) Lack of certified professionals Lack of accredited programmes and training institutions
Policies and regulations	Loss of trust No legal certainty	Coordination of ministries and units in the development of policies Ensure regulation's availability and clarity
Digital infrastructure	Unable to conduct efficient and effective business Unable to compete in global market	Lack of a uniform high-speed internet connection Scalable e-payment alternatives (other than credit cards) Digital access divide (i.e. urban vs. regional)
Global/ international environment	Unable to join global market	Adoption of open, international, industry, and technical standards for data exchange and systems interoperability Alignment with the ASEAN and relevant convention, e.g. ASEAN Network Security Action Council, International Telecommunication Union (ITU), APEC Privacy Framework Alignment with bilateral and multilateral trade agreements, e.g. the Indonesia–Australia Comprehensive Economic Partnership Agreement

Developing human capital and capacity in cyber security

Online security is focussed on the protection of e-commerce assets from unauthorised access, use, alteration, or destruction. When consumers conduct online transactions, they need to know that their online transactions are trusted and safe, and that they will enjoy the same legal protection as they do when dealing with traditional businesses.

Three human capital and capacity challenges potentially impedes the growth of e-commerce in Indonesia: perceptions, culture and skills. A study based on a survey of over 600 respondents (Rofiq 2012) found that Indonesian e-commerce customers' are highly influenced by perceptions of cyber fraud. Specifically, customers who have experienced cyber fraud incidents are less likely to engage in online purchases. Ensuring therefore that customers have positive experiences and perceptions toward cyber fraud are crucial for building overall confidence in e-commerce transactions. The same study also identified that in addition to promoting a positive experience, it is also important to educate customers on how systems security works and appropriate behaviours when completing online transactions as well as the importance of increasing support for governments and other relevant agencies in developing a safe e-commerce environment.

The second challenge to e-commerce growth is the low level of urgency regarding cyber security. Indonesian 'culture' is often cited as the primary threat to the cyber security discourse, especially with regards to the issues of integrity and confidentiality of information, making citizens the most vulnerable element. Awareness of cyber security threats and digital literacy education should thus be a priority in the development of the cyber security culture of Indonesian business and community.

A shortage of skilled workers is the third challenge. Austrade's ASEAN Market Insights (2019) reports that Indonesia faces a critical shortage of cyber security professionals. According to the Indonesian government, the digital industry needs to skill-up 600,000 workers a year to support business IT functions. However, the current Indonesian training system has weak linkages between government, industry, and education providers. Further, with the growing interest in this area, employers are expressing strong support for deeper collaboration between government, industry, and education providers to strengthen the fledgling training system.

Indonesia's President Joko Widodo has made human capital development a major priority for the next five years. The president has outlined under his agenda, the importance of creating work-ready graduates, and strengthening the training links between industry and education. Critical to graduates employability and industry linkages is developing curriculum based on international standards. Education and training systems need to adopt curricula that conform to global standards and produce graduates with skills and competencies that match the needs of employers and industry. Adopting (?) global standards based on schemes such as cyber security education (e.g. CSEC2017 - Cyber Security Education Curriculum) and including it in the job descriptions and roles (e.g. NICE 2.0) must be followed to address the need of knowledge and skills for the cyber security workforce. However, navigating through all these schemes has not been easy. Hudnal (2019) mapped the CSEC, CAE-CD, and NICE 2.0 schemes and argued that converging these in the creation of a Cyber Security Body of Knowledge would reduce the existing duplication of contents and deliver an integrated cyber security framework – an effort that is currently being undertaken by ICT professional associations, such as the Australia Computer Society (ACS).

Development like this should be closely monitored and, when relevant, adopted to benefit programme development in Indonesia's training and education, thus ensuring relevancy and up-to-date cyber security curricula and training modules.

Cyber security policies and regulations

Although Indonesia's cyber security policies and regulations have existed for many years, Rizal and Yani's (2016) study of cyber security in Indonesia provides a picture of a complex governance system, multi-sectorally structured, comprised of many players, and lacking coordination. Governments, universities and ICT communities, and the private sector (e.g. banking and oil companies) have all played various roles in the implementation of cyber security initiatives, but the major ministries that have direct cyber security responsibilities include the Minister of Communication and IT (Kominfo), Minister of Defence, and National Cyber and Encryption Unit – Badan Siber dan Sandi Negara (BSSN), which provides a direct report to the President. Having a coordinated approach in the development of relevant ICT policies and regulations is critical in such an environment.

In the e-commerce and online sector, policy and regulatory responsibilities also extend to the Ministry of Cooperatives and Small and Medium-sized Enterprises, Ministry of Trade (Kemendag), and Ministry of Industry (Kemenperin). Accordingly, inter-institutional coordination is desperately needed to ensure an optimal cyber defence for the country as well as the growth of effective online business activities.

Digital infrastructure

Poor digital infrastructure has been recognised as a major impediment to e-commerce in Indonesia. McKinsey (2016) predicted that the data traffic would increase six-fold in 2020, although Indonesia's IT spending lags behind that of many of its peer countries. In e-commerce, a major obstacle that inhibits the progress of e-commerce is network infrastructure (internet is cheap, but the quality is poor). In 2019, however, the Indonesian president vowed to improve support to help realise the digital economy through digitalisation of various processes, including electronic payment systems.

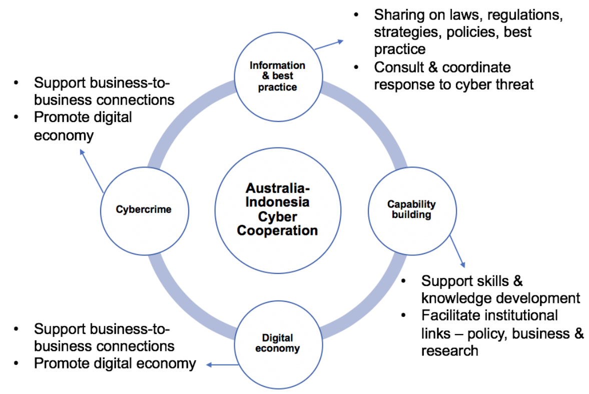
This indicates that significant investments might be made in ICT-related infrastructure in the next couple of years.

The digital divide is another issue relevant to Indonesia's e-commerce. While there has been rapid advancement of internet use in urban areas, the country's internet penetration remains low – around 25–35 per cent – which is one of the lowest rates in South East Asia. Moreover, the internet in Indonesia is characterised by low speed and limited coverage of electronic systems (Azali, K, 2017). In addition to the level of access, geography, gender, education, socio-economic status, and age are other factors contributing to Indonesia's digital divide. According to a recent polling study conducted by the Indonesian Internet Providers Association, the highest numbers of internet users are concentrated in Java (55 per cent) and Sumatra (21 per cent). Recent government policies and investments aimed at boosting internet penetration – especially geographical reach, speed, and quality access – in eastern Indonesia is beginning to address the issue (Oxford Business Group 2019).

Global/international environment

E-commerce extends beyond the boundaries of a single country, as cross-border trade transactions dominate the business activities. To facilitate this, the harmonisation of data, use of global standards, harmonisation of customs regulations, and various trade agreements need to be in place. Indonesia, as part of ASEAN and APEC, has been involved in the various standards and interoperability cross-border data flow and exchange agreements (e.g. Memorandum of Understanding of the ASEAN), but it needs to play an even larger role.

Figure 3 Indonesia-Australia Cyber cooperation framework


Australia-Indonesia Cyber Cooperation
Information & best practice
• Sharing on laws, regulations, strategies, policies, best practice
• Consult & coordinate response to cyber threat
Capability building
• Support skills & knowledge development
• Facilitate institutional links – policy, business & research
Digital economy
• Support business-to-business connections
• Promote digital economy
Cybercrime
• Support business-to-business connections
• Promote digital economy

In 2018, Indonesia entered an MOU with Australia on cyber cooperation to promote partnerships and provide a framework of cooperation on cyber issues (2018). Figure 2 provides a summary of this framework which covers the area of information sharing, capacity building and strengthening connection, digital economy, and cybercrime. Furthermore, Bilateral agreements, such as IA-CEPA (Indonesia–Australia Comprehensive Economic Partnership), should become a catalyst for cross-border e-commerce and trade facilitation.

Conclusion

A stronger and more robust Indonesian digital economy could be achieved through the creation of a safer and trusted e-commerce environment. Two initiatives that need to be implemented urgently and more effectively are (i) increasing citizens' cyber security awareness and (ii) addressing the shortage of cyber security professionals. While the former involves ensuring the right culture and attitude toward the digital economy, the latter also relates to recognising and opening the talent pool (e.g. recruiting and encouraging women into the industry).

Indonesia's policies and regulations will need some strengthening. As Chairil (2019) pointed out, these regulations are currently limited to electronic transactions only and do not cover issues relevant to e-commerce governance nor the government's roles in the cyber security system. Hence, it is important to fast-track the development of these laws and regulations.

Finally, having a reliable digital infrastructure, including options for digital payments (other than credit cards) and inclusive digital access, is necessary to ensure a sustainable and effective digital economy in Indonesia.

References

Asia Pacific Foundation of Canada (2018). 2018 Survey of entrepreneurs and MSMEs in Indonesia: Building the capacity of MSMEs through human capital, Asia Pacific Foundation of Canada - https://apfcanada-msme.ca/sites/default/files/2018-10/2018%20Survey%20of%20Entrepreneurs%20and%20MSMEs%20in%20Indonesia_0.pdf

AUSTRADE (2019). Cyber security opportunities in the Asean region. Singapore, AUSTRADE.

Azali, K. (2017). Indonesia's divided digital economy, Perspective, Yusof Ishak Institute ISEAS, No. 70 - https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2017_70.pdf

Chairil, T (2019). Cyber security for Indonesia: what needs to be done? The Conversation. May 9th

Das, K., et al. (2018). The digital archipelago: How online commerce is driving Indonesia's economic development, McKinsey & Company - https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Asia%20Pacific/The%20digital%20archipelago%20How%20online%20commerce%20is%20driving%20Indonesias%20economic%20development/FINAL_The-digital-archipelago-How-online-commerce-is-driving-Indonesias-economic-development.ashx

Hudnall, M. (2019). Educational and Workforce Cyber security Frameworks: Comparing, Contrasting, and Mapping. Computer **52**(3): 18-28.

Nugraha, L. K. and D. A. Putri (2016). Mapping the Cyber Policy Landscape: Indonesia. no. November.

Oxford Business Group (2019). Indonesia target internet penetration boost, Indonesia Country Report - https://oxfordbusinessgroup.com/analysis/connecting-nation-boosting-internet-penetration-rate-key-objective

Rizal, M. and Y. Yani (2016). Cyber security Policy and Its Implementation in Indonesia. Journal of ASEAN Studies **4**(1): 61-78.

Rofiq, A. (2012). Impact of cyber fraud and trust of e-commerce system on purchasing intentions: analysing planned behaviour in Indonesian business, University of Southern Queensland.

2016. Australia Cyber Security Strategy. Commonwealth Department.

2018. Survey of entrepreneurs and MSMES in Indonesia: Building the Capacity of MSMEs Through Human Capital. Asia Pacific Foundation of Canada.

2018. Memorandum of Understanding between The Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation. *In:* (DFAT). Bogor.

2019. Australia Cyber security Guide for Small Business. October. https://www.cyber.gov.au/publications/small-business-cyber-security-guide (accessed 21 October 2019)

2019, Digital 2019 Indonesia, We are Social. https://datareportal.com/search?q=Indonesia

Advancing An International Cyber Duty Of Care For Cyber Weapons

By Jonathan Lim and Ej Wise, EJ Wise Lawyers, Melbourne, Australia.

Introduction

The formation of a cyber duty of care vis-à-vis state and non-state actors, addressing instances of negligent or reckless practice - contributing to the widespread release of cyberweapons into the wider cyberspace environment and their ensuing devastation of modern digital infrastructure – must be entrenched into international law.

The creation and mass proliferation of cyberweapons by state actors has given rise to an increasingly precarious international cyber-threat environment - one where the reckless use and misplacement of cyberweapons by states, and their theft by hostile actors, presents a severe and collective threat to the national critical infrastructure of nation states and the wider cyberspace ecosystem.

The codification of a cyber duty of care concerning cyberweapons demands the coordinated effort of multilateral institutions, weapons manufactures, and end-users of such weapons – to avert the possibility of a cyber arms race, reduce the likelihood of conflict in cyberspace, and safeguard the developing right to internet access. [i]

Background

The commentary to Rule 103 of the Tallinn Manual 2.0 defines cyber weapons as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack." [ii] [iii]

The types of cyberweapons of concerned involve those specifically designed, used and sold by governments and private companies - able to penetrate networks and systems, even isolated and protected systems, to autonomously inflict the greatest amount of harm on the target. [iv] This circumstance has been advanced as the result of the increasing degree of geopolitical competition over cyberspace – with states adopting an increasingly aggressive stance of conducting offensive cyberattacks to achieve strategic and tactical objectives. [v] This is predicated on the significant benefits wrought by cyberweapons for its users - with cyber weapons being cheap and widely available, acting as a force multiplier for militarily inferior nations, and lending its user an air of plausible deniability. [vi]

Indeed, the use of cyberweapons by rogue states, such as North Korea, has allowed them to garner significant economic resources and influence global affairs. [vii] [viii] Similarly, the developing cross-proliferation of cyberweapons into the hands of cyber criminals has substantially multiplied the hazards of the cyber threat landscape – with cyberweapons sold for up to USD$50 million on the dark web. [ix]

The significant destructive potential of cyberweapons has given rise to calls by international commentators to classify them as a Weapon of Mass Destruction - given the potentially indiscriminate nature of such weapons, its ability to permanently damage critical infrastructure and other key assets of society, and its likelihood to cause mass injury and death rivalling the toll of a nuclear, chemical or biological weapon. [x] [xi]

While this existing environment has prompted a growing number of cybersecurity experts contend that companies that write computer software should be held liable for damages caused by exploits since defects in their software created the opportunities for those exploits.[xii] However, substantial legal uncertainties surround efforts to establish this liability regime.

Context

While current international efforts have failed to produce an enforceable codification of any type of norm concerning cyberweapons, there have been several notable forays into this internationally -

including efforts within the creation of the Tallinn Manual 2.0, those made by the United Nations (UN), and supplementary multilateral forums.

The Tallinn Manual represents an influential academic resource in understanding the current application of western international law norms to cybersecurity challenges. The manual was predicated by an alleged Russian-backed cyberattack on Estonian government institutions and state infrastructure in 2007. [xiii] The manual is the product of a group of international scholars convened by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia between 2009 and 2012. The first 2013 manual focused on crafting international customary practice surrounding severe cyber operations that violate the prohibition on the use of force, or entitle states to self-defence, in international relations. [xiv]

Consequently, Tallinn Manual 2.0 [xv] in 2017 served as a revision, as a non-binding comprehensive guide for policy advisors and legal experts on how existing international law applies to cyber operations – centred on the common cyber incidents that states encounter on a day-today basis which fall below the thresholds of the use of force. Herein, Rule 14 of the Manual covers intentionally wrongful cyber acts, outlining that a state bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.

Secondly, the UN has undertaken several measures via its subsidiary bodies in regulating the use of cyberweapons. Firstly, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security produced several reports in 2010, 2013 and 2015 on a global framework for cyber-stability. This in turn precipitated the UN General Assembly's unanimous adoption of Resolution 70/237 in 2015 – in which it called upon Member States to be guided in their use of ICTs by the 2015 GGE report.[xvi]

UN Secretary-General António Guterres has also prioritised the promotion of a peaceful ICT-environment, in launching his Agenda for Disarmament in May 2018.[xvii] In outlining that "malicious acts in cyberspace are contributing to diminishing trust among States" - Guterres included two action points on cyber in the implementation plan of the Agenda for Disarmament – focused on contributing to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace, and in fostering a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace. This was further observed through the UN Secretary-General's submission on Resolution 73/27 [xviii] and Resolution 73/266, [xix] which concluded on 15 May 2019. The contents of such submissions will be included in the 2019 annual report of the Secretary-General on Developments in the field of information and telecommunications in the context of international security.

Finally, the international community has also undertaken efforts, independent of the UN, in addressing the dangers posed by cyberweapons. This was illustrated during the November 2018 Paris Peace Forum,[xx] where 51 member states signed the Paris Call for Trust and Security in Cyberspace ('Digital Geneva Convention'). [xxi] The agreement represents the most recent coordinated effort by the international community to agree on a set of international rules for cyberspace. However, with Australia, US, UK, Russia, China, Iran, Israel and North Korea refusing to participate - the absence of leading cyberspace actors under the pact indicates that additional efforts must be made in promoting transparency and confidence building measures. Consequently, further talks on cyberweapons are anticipated during the upcoming Paris Peace Forum in November 2019. [xxii]

Australia's Offensive Cyber Capabilities

Where the Tallinn Manual and its contentions on cyberwarfare has been linked to the NATO doctrine on information operations, the content and substance of the Manual continues to be pertinent to Australia's military offensive cyber capabilities and its conduct within the area of cyber warfare. [xxiii]

In April 2016, then-Prime Minister Malcolm Turnbull made the first public disclosure of Australia's capability for offensive cyber military operations. Herein, Turnbull emphasized Australia's compliance under international law in emphasizing that 'The use of such a capability is subject to stringent legal oversight and is consistent with our support for the international rules-based order and our obligations under international law.' [xxiv]

Consequently, it has been advanced that users of Australia's cyber operations capability take compliance with both domestic and international law extremely seriously – having adhered to a set of core principles which appear closely aligned with the Rules of the Tallinn Manual and Just War Theory in its use: [xxv]

1. Necessity – In adhering to Rule No.26 (Necessity) in ensuring that an operation is necessary to accomplish a legitimate military or law enforcement purpose;

2. Specificity – Concerning Rule 111 (Indiscriminate attacks) in ensuring that an operation is not indiscriminate in who and what it targets;

3. Proportionality – Concerning Rule 72 (Necessity and proportionality) in ensuring the operation is proportionate to the advantage gained; and

4. Harm - Concerning Rule 72 (Necessity and proportionality) in considering whether an act causes greater harm than is required to achieve a legitimate military objective.

Consequently, Australia's offensive cyber operations are further subject to the Australian Signals Directorate's existing legislative and oversight framework - including independent oversight by the Inspector-General of Intelligence and Security. This presents a complex system of checks and balances on the use of such capabilities by the Australian Defence Force (ADF), one which is increasingly being called into question given its potential policy hinderance for the ADF in bridging the gap between strategic intent and operational and tactical applications. [xxvi] [xxvii]

Case Examples

Where former commander of the US Strategic Command James Ellis notes that the current strategic thinking on cyber conflicts is "like the Rio Grande [River], a mile wide and an inch deep" - [xxviii] this encapsulates the severe lack of hindsight demonstrated by cyberweapon manufacturers and sellers.

The most prominent example of a cyberweapon having been stolen, repurposed, and used to devastating effect was evident during the infiltration and theft of 300 GB of data - containing numerous top-secret cyberweapons - from the US National Security Agency (NSA) by the hacking group the "Shadow Brokers" in April 2016. [xxix] This was followed by the Shadow Brokers auctioning off the cyberweapons on the dark web, selling NSA acquired hacking tools to an undisclosed number of buyers for between $680,000 to $580 million. [xxx]

In the aftermath of the NSA Hack, their cyberweapons have been repurposed and used by cyber criminals and state actors on numerous occasions. This was observed during the global WannaCry ransomware attack on May 2017, where hackers used a modified version of NSA's stolen worm-like EternalBlue SMB exploit in an attack affecting over 200,000 victims across 150 countries – impacting computers in healthcare across the UK, USA and Australia. [xxxi] [xxxii]This was further reflected during the July 2017 NotPetya ransomware incident, which also used the NSW EternalBlue SMB exploit, resulted in over USD$10 billion in damages across numerous transnational companies – including Merck, FedEx, Saint-Gobain and Maersk. [xxxiii] [xxxiv]

NSA tools from the Shadow Brokers group were also connected to a series of attacks conducted by the Chinese hacking group APT3 between 2016 to 2017, where Chinese hackers used tweaked versions of "Eternal Synergy" and "Double Pulsar" in their attacks on US allies. [xxxv] [xxxvi] NSA cyberweapons also subsequently appeared during a cyberattack on the US city of Baltimore on 7 May 2019, where 10,000 government email accounts were targeted by a ransomware attack utilising the NSA malware tool EternalBlue – disrupting real estate sales, water bills, health alerts and other essential services. [xxxvii] [xxxviii]

Further, the public release of the Vault: CIA Hacking Tools by Wikileaks on 7 March 2017 resulted in the reckless disclosure and dissemination of the source code for numerous hacking tools used by the agency. [xxxix] The reconstruction, retooling, and manipulation of the source code for these tools by researchers has enabled the creation of specialist cyber-espionage weapons, [xl] and spurred continuing public and industry concerns over a looming wave of criminal cyber innovation and offensive cyber operations by adversarial state actors. [xli]

Israel represents one nation active in the development and sale of cyberweapons, and whose increasingly lax proliferation of cyberweapons presents an elevated threat to cyberspace. This was highlighted on 22 August 2019, when the Israeli Ministry of Defense reported its retrospective easing on export rules on offensive cyber weapons starting in 2018. The "marketing-licence exemption" permits companies to obtain exemptions on marketing licences for the sale of some products to specific countries - resulting in a speedier approval process for the sale of cyber weapons internationally. [xlii]

Analysis

The formation of a cyber duty of care for the manufacturers, sellers and end users of cyber weapons is important in precluding their theft and release into cyberspace and serves several purposes pertinent to the minimisation of public harm and the maintenance of international security.

Firstly, it holds the manufacturers of cyber weapons and responsible state actors accountable for the damages caused by their cyberweapons - thereby compelling a thorough consideration of the principles of proportionality under Just War Theory by any subsequent state-actor seeking the development and sale of such cyberweapons within the wider cyber ecosystem.

Secondly, it regulates the production and spread of cyber weapons – limiting the destructive capability of such weapons between state actors, and preventing such items from falling into the hands of non-state actors and terrorist groups. One example may be drawn from the results of the 1987 Intermediate-Range Nuclear Forces Treaty, which helped to regulate the volume of nuclear-capable weaponry in circulation and prevent an arms race between the between the US and Soviet Union. [xliii]

Finally, the establishment of an international cyber duty of care promotes the maintenance of peace, security, and stability in the international system. Establishing such a duty within international law simplifies the formation of a dispute resolution system, clarifies responsibility in incidents involving cyberweapons, minimises the potential for civilian casualties, and precludes the escalation of conflicts.

International law is made largely on a decentralised basis by the actions of the 192 States which make up the international community. Article 38 of the ICJ Statute identifies five sources – including treaties between states, customary international law, general principles of law recognised by civilized nations, and judicial decision and writings of "the most highly qualified publicists." [xliv]

The basis for establishing a cyber duty of care for cyberweapons may thus be pursued via the collective efforts of assorted international organisations, and the extension of existing responsibilities under a state's domestic laws – in the fostering of an *opinio juris* on the proliferation and use of cyberweapons. From this, the formation of a cyber arms control treaty represents a gateway to the eventual formation of a broader cyber duty of care concerning rogue cyberweapons. [xlv]

Indeed, precedent may be drawn from influential ICJ cases, among which includes the 1986 case *Nicaragua v. US* – which provided clarification on what constitutes an "armed attack", and held that "between independent states, respect for territorial sovereignty is an essential foundation of international relations." Henceforth, it may be established that hostile cyber operations directed against cyber infrastructure located on another state's territory constitute, inter alia, a violation of that state's sovereignty. [xlvi]

Conversely, the international community and the UN may simultaneously address the regulation of cyberweapons from the perspective of human rights. This may involve Article 17 of the International Covenant on Civil and Political Rights [xlvii] - directly appealing to the Special Rapporteur on the right to privacy to examine, monitor, advise, and publicly report on the adverse impact of cyber weapons on an individual's right to internet access. [xlviii] This may further elicit the issuance of a General Comment by the Human Rights Committee on the Article 17 and its connection to the adverse impacts of cyber weapons. [xlix]

Simultaneously, the international community may build upon the concept of the right to internet access in restricting the production and use of cyberweapons by state actors. In June 2016, the UN Human Rights Council passed a non-binding resolution which emphasized the importance of internet access for the fulfillment of human rights under Article 19 of the Universal Declaration of Human Rights. [l] The resolution called for states to adopt measures towards universal access to the internet, and specified that heavy restrictions on access to the internet should be interpreted as a violation of human rights. [li] Such multilateral efforts by the UN may also form the basis for the future formation of an optional protocol to the International Covenant on Civil and Political Rights. [lii]

Recommendations

Accordingly, the consensus, formation, and enforcement of a cyberweapons cyber duty of care by state-actors and NGOs throughout the international community – either in international customary practice of as a codified set of laws - must consider the following factors in attaining feasibility.

Firstly, the international community must determine enforcement measures and penalties concerning the production, sale and use of non-kinetic weaponry. For example, the imposition of an order to remediate every affected citizen/nation/business by the international community in the aftermath of a cyber incident would have a high prohibitive value.

Secondly, the creation of international customary law drawn from existing functional legal frameworks. This may be premised on the repurposing of US laws under the EAR and ITAR to form the basis for an *opinio juris* concerning the duty of care in relation to cyberweapons. [liii]

Thirdly, establishing an agreed means of accepted attribution, or the assumption of attribution, in relation to the implicated cyberweapon. The increased speed at which targeted states' push the attribution of, and indictments for, cyberattacks over the past several years highlights the persisting importance of sending a public message to the attackers, while also promoting accountability and transparency in the international order. [liv]

Fourthly, agreements over what constitutes both permitted and prohibited cyberweapons. This may encompass cyberweapons whose use would, by definition, produce superfluous injury or unnecessary suffering upon the intended target. Such requires specifying the nature and effect of these banned cyberweapons, crafting a consensus among state actors, and enshrining this common classification into international law.[lv] [lvi]

Matters for future discussion

Firstly, unlike the use of chemical and nuclear weapons, part of the nature of cyber weaponry is its secrecy. Forming a register of cyber weapons in order to restrict, limit, or reduce their use is counter to the stealth nature of the weapon. There has been discussion already that the use of a cyber weapon is often delayed owing in part to the huge investment in its creation and that once deployed it is able to be examined and a great deal learned about the actor who produced it, their general capability, sophistication and can make future detection and attribution easier.

"While some overt offensive cyber use adds to deterrence, at the same time it creates a sort of cyber weapons paradox between overt cyber deterrence and covert cyber usefulness because any overt use can render the weapon useless. The paradox also exists because of the nature of cyber weapons themselves."[lvii]

Secondly, ASPI experts argue that the scale and seriousness of [cyberattack] incidents should be based upon measuring the ultimate consequences of an incident and the economic and flow-on *effects.*[lviii] Amongst their recommendations are limitations on collateral damage (that cyber weapons should be targeted: already a requirement in the conduct of armed conflict); increased state transparency; and improved accounting of the damage which has occurred. The practical implementation of such recommendations is for future discussion.

Conclusion

The terms of state-vs-state conflict under international law have been limited by a variety of international agreements, state practice and international norms. It is incumbent upon each-and-every state-actor capable of manufacturing, hosting or trading in cyber weapons to collectively agree on those cyberweapons whose use is simply unacceptable due to their unknowable or profound effects. The utility of the recommendations proposed in this document to the international order and cyberspace is multifold.

Firstly, the acceptance of these recommendations signals a positive movement towards accepted state practice, and an assured level of cyber-safety for citizens and public organisations around the globe.

Secondly, such recommendations will address the increase in cyber incidents – including the threat of cybercrime, increased blurring of the lines between cyber-crime/espionage/conflict, and will scale the difficulties in distinguishing between state and non-state actors. Adding to this will be increasing service and delivery interruptions to citizens, and obfuscation of what individuals believe they 'see' on the news, 'hear' on their phones, and 'experience'.

Third, based upon the historical development kinetic warfare treaties, international law and jurisprudence – achieving a tangible agreement between nation states on recommendation No.1 (*enforcement measures and penalties)* and recommendation No.2 (*agreed prohibited cyber weapons)* represents a definitive trend within international relations over the next decade.

Fourth, the Australian government is in a unique position to spearhead these initiatives – as a developed nation, a member of the Five-Eyes Community, and a state with an established offensive cyber capability. With the increasing reliance of Australians upon IoT devices, the Government must seize the initiative to contribute to the 2019 Paris Peace Accord, and the continued efforts of the UN and ICRC, in highlighting the broad threat posed by cyberweapons.

It is inevitable that certain state actors (i.e. North Korea, Russia, China, Iran) will continue to hinder and circumvent the development of an international duty of care concerning cyber weapons for the foreseeable future. This is understandable given the continuing gap in capability between such countries versus countries which possess advanced capabilities in cyber operations (i.e. the US), and the cost-effective nature of non-kinetic cyber operations versus kinetic attacks. [lix]However, such attempts to hinder the codification of restrictions on cyber weapons into international law does not preclude its adoption into international customary practice. [lx]

Regardless, the continued absence of international norms surrounding the development of offensive cyber capabilities and weaponry will enable states to utilize such capabilities without any mindfulness to international law and norms. In this context, and in promoting multilateral transparency and confidence building measures, it is imperative that the international community collectively approaches the issue of cyber weapons with the utmost transparency – to ensure that there is a clear and open conversation around the use and consequences of offensive cyber capabilities. [lxi]

[i] Catherine Howell and Darrell M. West, ‘The internet as a human right’ on Brookings Institution (7 November 2016) <https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/>.

[ii] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 452.

[iii] Denis Miralis, ‘What are Cyber Weapons?: Some Competing Definitions’ on Lexology (28 September 2018) <https://www.lexology.com/library/detail.aspx?g=65179269-c85e-4253-a9a3-5d9ba1c9c906>.

[iv] David Wallace, ‘Tallinn 2018Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis’ on NATO Cooperative Cyber Defence Centre of Excellence (2018) <https://ccdcoe.org/uploads/2018/10/TP-11_2018.pdf>16.

[v] Stratfor, ‘The U.S. Unleashes Its Cyberweapons’ on Stratfor (5 July 2019) <https://worldview.stratfor.com/article/us-unleashes-its-cyberweapons-iran-russia-china-cyberwar>.

[vi] Sue Halpern, ‘How Cyber Weapons Are Changing the Landscape of Modern Warfare’ on The New Yorker (18 July 2019) <https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare>.

[vii] Christopher A. Bartos, ‘Cyber Weapons Are Not Created Equal’ on US Naval Institute (June 2016) <https://www.usni.org/magazines/proceedings/2016/june/cyber-weapons-are-not-created-equal>.

[viii] Michelle Nichols, ‘North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report’ on Reuters (6 August 2019) <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX>.

[ix] Alison DeNisco Rayome, ‘Programmer tried to sell cyberweapon on dark web for $50M: Reminder to secure employees’ on Tech Republic (5 July 2018) <https://www.techrepublic.com/article/programmer-tried-to-sell-cyberweapon-on-dark-web-for-50m-reminder-to-secure-employees/>.

[x] Jeremy Straub, ‘A Major Cyber Attack Could Be Just as Deadly as Nuclear Weapons, Says Scientist’ on Science Alert (18 August 2019) <https://www.sciencealert.com/a-major-cyber-attack-could-be-just-as-damaging-as-a-nuclear-weapon>.

[xi] Scheiner on Security, ’Cyberweapons vs. Nuclear Weapons’ on Scheiner on Security (22 July 2016) <https://www.schneier.com/blog/archives/2016/07/cyber_weapons_v.html>.

[xii] Paul N.Stockton and Michele Golabek-Goldman, ‘Curbing the Market for Cyber Weapons’ (2013) 32 *Yale Law & Policy Review* 242.

[xiii] Stephanie MacLennan and Naomi O’Leary, ‘Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game’ on Centre for International Governance Innovation (26 October 2017) <https://www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game>.

[xiv] Jill D. Rhodes and Robert S. Litt, *The ABA Cybersecurity Handbook – Second Edition* (American Bar Association, 2018) 254.

[xv] N. Schmitt, above n2, 79.

[xvi] United Nations, ‘UNGA Resolution 70/237: Developments in the field of information and telecommunications in the context of international security’ on United Nations (30 December 2015) <https://dig.watch/instruments/unga-resolution-70237-developments-field-information-and-telecommunications-context>.

[xvii] United Nations, ’Security our Common Future – An Agenda for Disarmament’ on United Nations (May 2018) <https://www.un.org/disarmament/sg-agenda/en/>.

[xviii] Developments in the field of information and telecommunications in the context of international security.

[xix] Advancing responsible State behaviour in cyberspace in the context of international security.

[xx] France24, ''Paris Call': 51 states vow support for global rules on cyberweapons' on France24 (12 November 2018) <https://www.france24.com/en/20181112-france-internet-paris-call-51-states-support-cybersecurity-rules-cyberweapons-peace-forum>.

[xxi] Ministry for Europe and Foreign Affairs, 'Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace' on Ministry for Europe and Foreign Affairs (12 November 2018) <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>.

[xxii] Shervin Taheran, 'France Calls for Global Cybersecurity' on Arms Control Association (2019) <https://www.armscontrol.org/act/2019-01/news-briefs/france-calls-global-cybersecurity>.

[xxiii] Katherine Murphy, 'Australia taking cyber fight to Isis, Malcolm Turnbull to confirm' on The Guardian (23 November 2016) <https://www.theguardian.com/technology/2016/nov/23/australia-taking-cyber-fight-to-isis-malcolm-turnbull-to-confirm>.

[xxiv] Rohan Pearce, 'Cyber deterrent: PM talks up Australia's offensive capabilities' on Computerworld (21 April 2016) <https://www.computerworld.com.au/article/598443/cyber-deterrent-pm-talks-up-australia-offensive-capabilities/>.

[xxv] Fergus Hanson and Tom Uren, 'Australia's Offensive Cyber Capability' on ASPI (10 April 2018) <https://www.aspi.org.au/report/australias-offensive-cyber-capability>.

[xxvi] Ibid.

[xxvii] Christopher Wardrop, "Bridging the gap between cyber strategy and operations: A missing layer of policy" (2018) 204 *Australian Defence Force Journal* 61-69.

[xxviii] Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." (2018) 12(3) *Strategic Studies Quarterly* <www.jstor.org/stable/26481911> 91.

[xxix] Olivia Solon, 'Hacking group auctions 'cyber weapons' stolen from NSA' on The Guardian (17 August 2016) <https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group>.

[xxx] Jai Vijayan, 'Shadow Brokers Offers Database Of Windows Exploits For Sale' on DarkReading (10 January 2017) <https://www.darkreading.com/attacks-breaches/shadow-brokers-offers-database-of-windows-exploits-for-sale/d/d-id/1327867>.

[xxxi] Thomas Brewster, 'An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak' on Forbes (12 May 2017) <https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#2c426bf7e599>.

[xxxii] Reuters, 'Cyber attack hits 200,000 in at least 150 countries: Europol' on Reuters (14 May 2017) <https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX>.

[xxxiii] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' on Wired (22 January 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

[xxxiv] Ian Thomson, 'Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide' on The Register (28 June 2017) <https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/>.

[xxxv] Nicole Perlroth and David E. Sanger, Scott Shane, 'How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks' on The New York Times (6 May 2019) <https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html>.

[xxxvi] Zak Doffman, 'China Set Traps To Capture Dangerous NSA Cyberattack Weapons: New Report' on Forbes (5 September 2019) <https://www.forbes.com/sites/zakdoffman/2019/09/05/secret-chinese-hacking-group-set-traps-to-steal-nsa-cyberattack-tools-new-report/#3643223b48ce>.

[xxxvii] Jared Keller, 'An NSA cyber weapon is reportedly being used against American cities by the very adversaries it was meant to target' on Task & Purpose (25 May 2019) < https://taskandpurpose.com/nsa-cyber-weapon-american-cities>.

[xxxviii] Emilio Iasiello, 'Government Responsibility and Leaked Cyber Weapons' on Technative (13 June 2019) <https://www.technative.io/government-responsibility-and-leaked-cyber-weapons/>.

[xxxix] Wikileaks, 'Vault 7: CIA Hacking Tools Revealed' on Wikileaks (7 March 2017) <https://wikileaks.org/ciav7p1/>.

[xl] Jeff Stone, 'A researcher made an elite hacking tool out of the info in the Vault 7 leak' on Cyberscoop (27 February 2019) <https://www.cyberscoop.com/vault-7-operation-overwatch-cia-hacking-tools-rsa-conference/>.

[xli] Nick Palmer and Moshe Ben-Simon, 'Vault 7 and the Coming Wave of Criminal Cyber Innovation' on Trapx (18 March 2017) <https://trapx.com/vault-7-and-the-coming-wave-of-criminal-cyber-innovation/>.

[xlii] Tova Cohen and Ari Rabinovitch, 'Israel eases rules on cyber weapons exports despite criticism' on Reuters (22 August 2019) <https://uk.reuters.com/article/uk-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUKKCN1VC0Y0>.

[xliii] Anant Saria, 'I Don't Want to Set the World on Fire: Abandoning the INF Treaty Could Spark a Global Arms Race' on Young Diplomats Society (6 March 2019) <https://www.young-diplomat.com/single-post/2019/03/06/I-Don%E2%80%99t-Want-to-Set-the-World-on-Fire-Abandoning-the-INF-Treaty-Could-Spark-a-Global-Arms-Race>.

[xliv] Christopher Greenwood, 'Sources of International Law: An Introduction' on United Nations (4 November 2008) <http://legal.un.org/avl/pdf/ls/greenwood_outline.pdf>.

[xlv] Martin Giles, 'We need a cyber arms control treaty to keep hospitals and power grids safe from hackers' on MIT Technology Review (1 October 2018) <https://www.technologyreview.com/s/612215/we-need-a-cyber-arms-control-treaty-to-keep-hospitals-and-power-grids-safe-from-hackers/>.

[xlvi] Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' (2014) 25(2) *Stanford law & Policy Review* 269-300.

[xlvii] United Nations Human Rights – Office of the High Commissioner, 'International Covenant on Civil and Political Rights' on United Nations (2019) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

[xlviii] United Nations Human Rights – Office of the High Commissioner, 'Special Rapporteur on the right to privacy' on United Nations (2019) <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

[xlix] United Nations Human Rights – Office of the High Commissioner, 'Human Rights Treaty Bodies - General Comments' on Untied Nations (2019) <https://www.ohchr.org/EN/HRBodies/Pages/TBGeneralComments.aspx>.

[l] Howell and West, above n1.

[li] Jesse Tomalty, 'Is There A Human Right To Internet Access?' on Philosophy Now (2017) <https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access>.

[lii] ESCR-Net, ‘Section 2: Improving Supervision of the ICESCR: an Optional Protocol’ on ESCR-Net (2019) <https://www.escr-net.org/resources/section-2-improving-supervision-icescr-optional-protocol>.

[liii] Trey Herr and Paul Rozenweig, ’Cyber Weapons and Export Control: IncorporatingDual Use with the PrEP Model’ (2015) 8 *Journal of National Security Law & Policy* 301-319.

[liv] Sally Cole, ‘Cyberattack attribution: Is it actually a deterrent?’ on Military Embedded Systems (15 May 2018) <http://mil-embedded.com/articles/cyberattack-attribution-it-actually-deterrent/>.

[lv] Rule 78. The anti-personnel use of bullets which explode within the human body is prohibited.

[lvi] e.g. The kinetic equivalent of exploding rounds does not require discussion of how the rounds are manufactured and instead focusses on the result of their use.

[lvii] Goines, Timothy M. “Overcoming the Cyber Weapons Paradox.” *Strategic Studies Quarterly*, vol. 11, no. 4, 2017, pp. 86–111. *JSTOR*, www.jstor.org/stable/26271635.

[lviii] Uren, Hogeveen and Hanson. ’Defining Offensive Cyber Capabilities’ on Australian Strategic Policy Institute. International Cyber Policy Centre (4 July 2018) <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities>.

[lix] Zak Doffman, ‘Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S.’ on Forbes (6 July 2019) <https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/#57c579ee42eb>.

[lx] Nele Achten, ‘New U.N. Debate on Cybersecurity in the Context of International Security’ on Lawfare (30 September 2019) <https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security>.

[lxi] Sandhya Sharma, ‘Australia concerned about offensive cyber warfare capabilities build up in Indo-Pacific’ on The Economic Times (4 September 2019) <https://economictimes.indiatimes.com/news/defence/australia-concerned-about-chinas-cyber-warfare-capabilities-in-indo-pacific/articleshow/70975958.cms>.