National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

APPRECIATING INFORMATION PROTECTION AND OPERATIONALIZED SOCIAL MEDIA AS A WICKED PROBLEM

Maj Jason Neufeld

JCSP 43 DL

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 43 AD

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

APPRECIATING INFORMATION PROTECTION AND OPERATIONALIZED SOCIAL MEDIA AS A WICKED PROBLEM

Maj Jason Neufeld

Word Count: 3335

Compte de mots: 3335

APPRECIATING INFORMATION PROTECTION AND OPERATIONALIZED SOCIAL MEDIA AS A WICKED PROBLEM

INTRODUCTION

Globalization, the proliferation of the internet and the expansion of cellular and satellite communications have allowed instant access to news and information to millions of people unlike ever before. The ability to not just communicate, but to govern through an application or an email has completely changed how we function as a society. Despite this, no matter how much faster or wider our messages travel, at the root are people, and their nature has not changed.[1] There remains a faction of society that will want to counter the state, right or wrong, they will take full advantage of the resources they have at hand.[2] Today those resources include global social media which is creating an equalization effect that allows a small group of determined individuals to influence and impact society on the same level as the institutions they oppose.

Until recently, protecting information has been, for the most part, something that remained behind the scenes, almost clandestine in nature. Carried out by specialists leaving the average user of information only expected to use basic principles and practices. Today, as we have become increasingly interconnected, technical solutions are just a small element of what is required to protect our most vital information.

---

[1]Colonel Glenn Voelz and Sarah Soliman. "Identity, Attribution, and the Challenge of Targeting in the Cyberdomain." Marine Corps University Journal Vol.7. No.1 (Spring 2016): 12.

[2] David Tayouri. "The Human Factor in the Social Media Security - Combining Education and Technology to Reduce Social Engineering Risks and Damages." *Procedia Manufacturing* Vol 3 (2015): 1097 https://ac.els-cdn.com/S2351978915001821/1-s2.0-S2351978915001821-main.pdf?_tid=6c3250ea-f680-4814-9916-ad924709614b&acdnat=1523685907_6896238ff7ac404a42980385e3de623d

The true dichotomy here is not just that the more we want to use social media and information systems the greater the risk we face, but we must also respect the equalization effect, and that the less we use social media and information systems, the greater the threat we face from current and future adversaries. This paper will examine both of these themes, information protection and the operationalization of social media. It will also demonstrate why this issue is a wicked problem by using Rittel's ten attributes of a wicked problem. Understanding that this is a wicked problem is important in order for planners, decision makers and practitioners to apply the correct models and tools to address the true nature of the challenge they face.[3]

INFORMATION PROTECTION

> *There is a fundamental change at the moment towards a data society. Everybody in the world is connected to each other and influenced by algorithms keeping us in our bubble. The environment we are living in is smarter than we are.*
>
> - Brigadier General Hans Damen, *Defence and Military Sector Conference 7 December 2017*

As the proliferation of information systems and technologies have grown, so too have the processes, systems, policies and programs designed to offer protection of our most vital pieces of information. In order to fully appreciate the nature of our problem, one must first understand just how complex information protection has become. This section will examine the current nature of information protection as it relates to defence and the human element.

The government of Canada defines Information Technology Security as the "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically

[3] Horst W.J. Rittel, and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4, no. 2 (June 1973): 160-161

stored, processed or transmitted information."[4] This definition has been expanded to include "the safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically."[5] These definitions are important as they help shape the technology side of information protection. An examination of Figure 1, which outlines the Information Security Map, gives us a good appreciation of just how complicated this is.

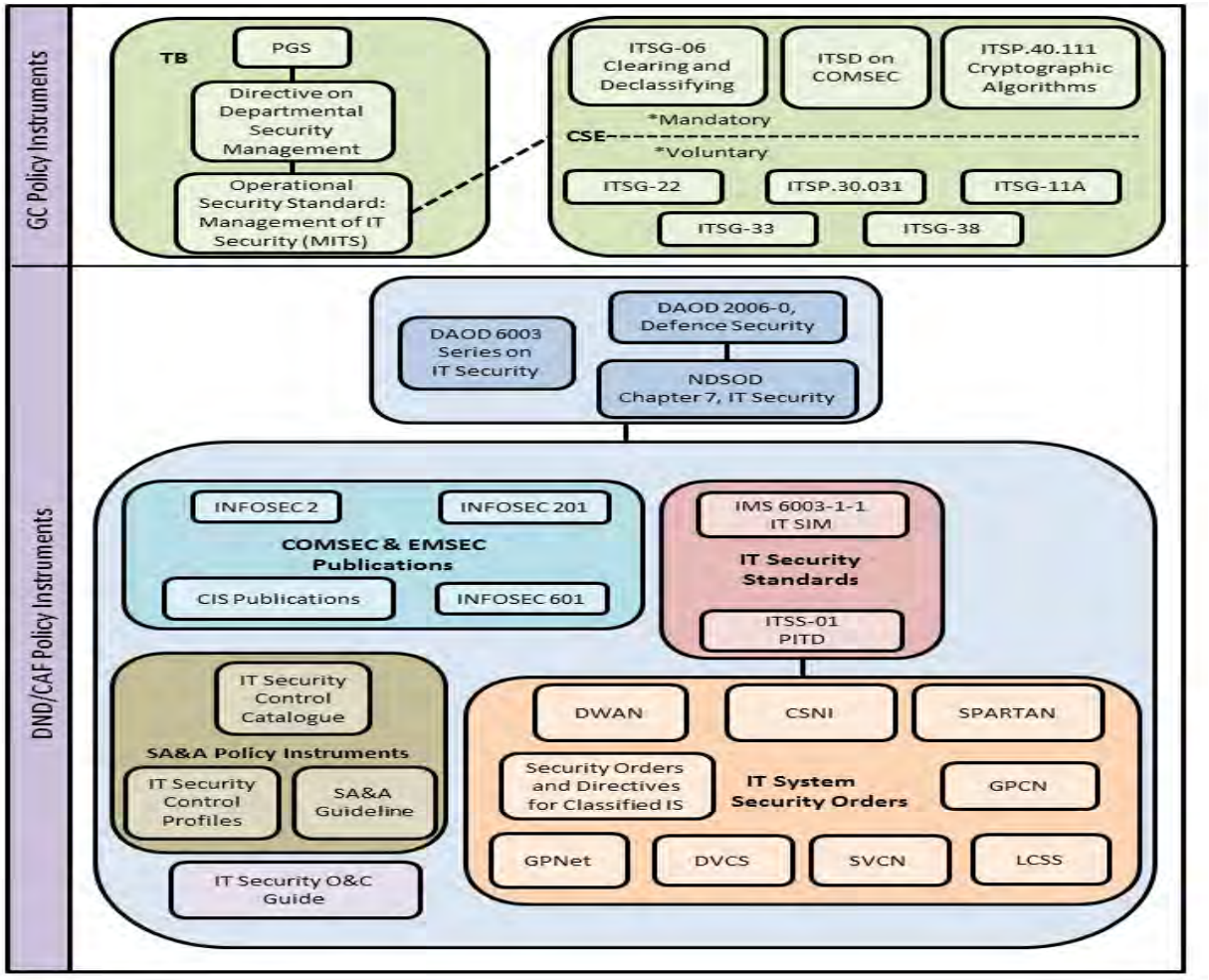

Figure 1 - Government of Canada and Department of National Defence/Canadian Armed Forces Information Security Map

Source: Canada. National Defence Security Orders and Instructions, Chapter 7, Information Technology Security, 3.

[4] Government of Canada. "Government Security Policy". Archived 7 Jun 2009, last modified 1 Feb 2002. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322

[5] Operational Security Standard: Management of information Technology Security (MITS) dated motivated 2004-05-31 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328

Because we do not operate on a single platform, the number and types of networks only serve to further complicate the picture, as the wide range of rules and policies are primary drivers behind how those networks are constructed and used. In some cases, such as with classified networks, the systems have been specifically built to satisfy the exigencies of the security policies. While in cases where networks have more persistent connectivity to the internet, the policies and standards are used to control the nature and use of the network in question. Put all of this together and we have a rather complex network of policies, directives, physical and virtual components that all need to work to together to protect the information and users.

As seen by the recent ransomware attacks, traditional threats such as viruses, hackers and malware remain, but they are by far not the only threat to be considered.[6] With globalization and the immediate access to the internet at all levels of society, the human element plays a much greater role in the overall threat profile and the associated information protection required.[7] Traditional information handling principles must be expanded to include the relationship and role of social media in how we conduct business. Firewalls and virus software will not protect the information if someone posts the locations and dispositions of troops in a twitter post.

We are now increasingly concerned with threats developed through *social engineering* that attack not just the systems but human trust.[8] *Cyberbullying*, *Phishing* and *Spear-phishing*, have been added to the lexicon of information security.[9] These elements of security are far less

---

[6] Khidzir, N.Z., A.R. Ismail, K.A.M. Daud, M.S.A.A. Ghani, and M.A.H. Ibrahim, Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements. ETPUB - Engineering and Technology Publishing. June 2016, vol.4, no.1, pp. 19.

[7] Tayouri. "The Human Factor in the Social Media Security…" 1097.

[8] Tayouri. "The Human Factor in the Social Media Security…" 1097.

[9] Nena Giandomenico. "What is Spear-phishing? Definition and Differentiating Spear-phishing from Phishing." Digital Guardian 27 June 2016. https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing Phishing and Spear-phishing are target attacks usually through carefully crafted emails sent to individuals in an attempt to steal sensitive information. Spear-phishing involves targeting a

prescriptive, relying very much on individual judgement, education and intelligence. With today's global interconnectivity, users are exposed almost on a persistent basis.

OPERATIONALIZED SOCIAL MEDIA

> *As a critical element within the information environment, social media provides a readily available means and conduit to attack and exploit the "temporal" dimensions of the modern battlefield*.
>
> - Nicholas Shallcross, Social Media and Information Operations in the 21st Century

We now live in an era where we have unprecedented access to not only vast amounts of information, but the ability to present, modify, obscure and broadcast this information to an audience never before experienced.[10] At the strategic layer, this allows governments to share and distribute their messaging to almost anyone, anywhere and instantaneously. A clear example of this is how the current President of the United States is governing his superpower as much through his twitter account as any other means. Social media is now being used on an unprecedented global level to influence world opinion immediately.[11]

Closer to home, a recent report showed that between January 2016 and March 2018, the Canadian Government spent more than $24 million on Facebook and Instagram ads, posts, and videos.[12] All of these efforts are deliberately planned uses of social media to reach a huge volume of people, to sway public opinion and influence the outcomes of any number of decisions. Social media has become the weapon of choice for opposition parties, federal

---

specific individual, usually within a company or organization. Whaling is a spear-phishing attack targeted against senior, high ranking individuals.

[10] Jack Barclay, *Social media growth threatens SF operations.* Jane's Intelligence Review (5 May 2016): 2, https://janes.ihs.com/Janes/Display/jir12142-jir-2016

[11] Terry Collings, "Trump's Itchy Twitter Thumbs Have Redefined Politics." C-Net 20 January 2018. https://www.cnet.com/news/donald-trump-twitter-redefines-presidency-politics/

[12] Teresa Wright, "Canadian government spending tens of millions on Facebook Ads, Sponsored Posts." Canadian Press Tues May 22, 2018. https://www.thestar.com/news/canada/2018/05/22/canadian-government-spending-tens-of-millions-on-facebook-ads-sponsored-posts.html

lobbyists, and special interest groups. One only needs to google Kinder Morgan to witness the power and influence that social media can have on political decisions and the provincial economies.[13] Throw in an expert opinion or even just celebrity interest and soon a small interest group is wielding tremendous power.

More than just a means to advertise and influence opinion, social networks and the internet at large are the means by which governments now operate. Contracts are solicited and awarded through automated websites; the Defence Acquisition Guide is available to the public highlighting all of the potential capabilities that defence is going to invest money into; even most military units now have their own internet presence, many with active and public Facebook accounts. All of this to allow instant and persistent access to government resources and to connect with those that have a role in the conduct of government.

Taking this down to the operational level, this ability to instantly reach the masses, even within a concentrated area of an operational environment, can play significant dividends. A simple example would be the ability to transmit critical information on evacuations, collection points, or recovery efforts. Where in the past soldiers in support of flood events would have to go door to door to reach individuals, the availability of social media is able to reach victims unlike ever before. Another good example was the RANA-FM radio station that was launched in 2007 as part of the information operations campaign in Afghanistan. This radio station, operated from Canada, was designed to specifically reach and influence Afghans in the 15-25 age group through a program of modern Afghan music, sports, news along with messaging from the

[13] Trish Audette-Longo, "Kinder Morgan Pipeline supporters and Detractors are Being Swarmed by Online 'Bots'." National Observer 20 April 2018. https://www.nationalobserver.com/2018/04/20/analysis/kinder-morgan-pipeline-supporters-and-detractors-are-being-swarmed-online-bots

Operational commander. [14] Today, this same effect can be achieved through a wide range of social media systems, with a fraction of the infrastructure.

Figure 2. Cpl Sebastien Leclerc standing on TV Hill in Kabul Afghanistan in 2004 demonstrates just how prolific radio and data communications have become in third world locations.

Source: Sgt Frank Hudec, Canadian Forces Combat Camera

State and non-state actors are using social media for offensive and defensive operations to tremendous effect. A prime example is the manipulation of social media trend algorithms in applications like Twitter and Facebook to change the significance of a given issue or event. By creating the appearance of a large vocal audience using both real and computer generated accounts, adversaries are able to create the illusion that an issue is trending higher than it really is. Many users of these applications rely on these trends lists to see what the most important or significant news items are. Through such activities, adversaries are able to disseminate their

[14] Canadian Broadcasting Company. "Canada's Radio Kandahar Goes to Air." CBC News (6 January 2007). http://www.cbc.ca/news/canada/canada-s-radio-kandahar-goes-to-air-1.654396

messages, real or otherwise, with a small number of trained personnel from the comfort of their own countries.[15]

For our own part, Social media is now one of the most lucrative environments for gathering data and intelligence. Images can be used to identify individuals and their associations, to track patterns of life and even locate their whereabouts. Through technical and psychological profiling, a target can be identified and tracked through a combination of systems they use, their internet habits, biometrics and who they connect with.[16] This new level of intelligence gathering and collection significantly changes how combat operations can be executed. Counterterrorism and counter-insurgency are as much about defeating the insurgency as it is about winning the social and mental war with the local populations. This takes careful messaging and counter-messaging.[17]

THE WICKED PROBLEM

It is easy to see from the previous sections that there is a complexity that exists within how we protect ourselves against the risks and threats and the benefits of being able to use technology and social media to disseminate messaging, conduct command and control and information operations while gaining critical intelligence and situational awareness. But is this dilemma so complex that it should be deemed, and subsequently treated as a wicked problem?

---

[15]Nicholas Shallcross, "Social Media and Information Operations in the 21st Century" Working Paper, University of Arkansas, February 2016. 5.

[16] Colonel Glenn Voelz and Sarah Soliman. "Identity, Attribution, and the Challenge of Targeting in the Cyberdomain." Marine Corps University Journal Vol.7. No.1 (Spring 2016): 10.

[17] Prier, Jarred. "The Command of the Trend: Social Media as a Weapon in the Information Age." Graduate thesis, Air University Maxwell Air Force Base, Alabama, June 2017. 31, 74. An American funded program called "Think Again Turn Away" was a failed attempt to establish a counter-messaging program using social media to against ISIS. It serves as an excellent example of how difficult and dangerous using social media can be if not executed correctly.

The following section will use Rittel's ten attributes of a wicked problem to both answer this question and gain an appreciation of where potential starting points lie with respect to finding a resolution.[18]

1. There Is No Definitive Formulation Of A Wicked Problem

There is no established framework from which commanders are able to understand the full spectrum of the problem. There is no situational map that is thrown up during the initiation phase of an operation that defines the full scope of the cyber battlefield. This is not simply because the problem is complex, but because the relationships and system-of-systems nature of social media, networks and people the problem set are always in a constant state of change.[19] The diversity of the information and its associated risks and vulnerabilities is persistently fluid. One would have to examine every single digital presence, friend or foe, and how those points of presence will respond to a given element of information stimulus just to start framing the scope of the problem. With the speed in which these responses will evolve, the full scope of the problem will never be realized before it changes.

2. Wicked Problems Have No Stopping Rule

There is no start or stopping point within the Cyber domain. The more one uses the systems, applications and networks the greater the potential vulnerabilities one faces.[20]

---

[18] Horst W.J. Rittel, and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4, no. 2 (June 1973): 161-167.

[19] Colonel Glenn Voelz and Sarah Soliman. "Identity, Attribution, and the Challenge of Targeting in the Cyberdomain." Marine Corps University Journal Vol.7. No.1 (Spring 2016): 13.

[20] Barclay, Jack, Social media growth threatens SF operations. Jane's Intelligence Review (5 May 2016): 2-3. https://janes.ihs.com/Janes/Display/jir12142-jir-2016

Conversely, the less one uses the cyber domain, the greater the advantage an adversary has when conducting information operations or propaganda campaigns.[21] In the modern age of social media and instant messaging, there is no opt-out option, nor is there a simple solution that allows complete governance. In the same way that there is no definitive solution to this challenge, there is no stopping point. As new technologies evolve, decision-makers must re-address all of the previously established variables and considerations. At no point does this stop.

3. There Are No Criteria For Correctness

There is no immediate discernable solution set, each situation will be unique, each decision maker will approach this problem differently, and any solution today may not work tomorrow. The growth of asymmetrical or hybrid warfare prevents the problem solver from choosing from a doctrinal solution set.[22] The commander may choose a particular option to address the symptoms of the problem, but he will not resolve the issue, and in some cases, he may be introducing or exacerbating other symptoms.[23] Restrict all of your information away from the internet you reach a much smaller audience. Increase the information distribution and you become increasingly vulnerable.

---

[21] Nicholas Shallcross, "Social Media and Information Operations in the 21st Century" Working Paper, University of Arkansas, February 2016: 9.

[22] Colonel Glenn Voelz and Sarah Soliman. "Identity, Attribution, and the Challenge of Targeting in the Cyberdomain." Marine Corps University Journal Vol.7. No.1 (Spring 2016): 17.

[23] Prier, Jarred. "The Command of the Trend: Social Media as a Weapon in the Information Age." Graduate thesis, Air University Maxwell Air Force Base, Alabama, June 2017: 74

4. There is No Immediate Test of the Quality of the Solution

The distribution of the audience, the mechanisms to receive and send information and the ability to manipulate information means that there is no mechanism to evaluate the success of a solution. For example, you can make more information available, but if you do not maintain the information, it quickly becomes obsolete and there is no method to measure if this was successful or not. Once implemented, the circumstances will change such that success criteria may be invalid. There is also no means to determine effectiveness. Once you decide on one potential solution there is a corresponding counter to it almost immediately, with the process restarting just as quickly. Without an ability to stop or start this process, there is no methodology to determine if you have been successful.

5. Every Solution to a Wicked Problem is a "One-Shot Operation"

The memory of the cyber domain is eternal and that once you choose one solution, it is there for all to see, use, redistribute and manipulate[24]. There are no mechanisms to stop a post after having been sent or a message from being stored or received. Tools can be applied in response to recognized threats or vulnerabilities, but this is all a reaction to the circumstances and the decisions that are implemented. Consider the impact that a single soldier can have on the public image or impression of an operation. Often referred to as the Strategic Corporal, the

[24] David Tayouri. "The Human Factor in the Social Media Security - Combining Education and Technology to Reduce Social Engineering Risks and Damages." *Procedia Manufacturing* Vol 3 (2015): 1097 https://ac.els-cdn.com/S2351978915001821/1-s2.0-S2351978915001821-main.pdf?_tid=6c3250ea-f680-4814-9916-ad924709614b&acdnat=1523685907_6896238ff7ac404a42980385e3de623d

comments or actions of even one individual can have a significant and irreversible influence on how the problem is treated.[25]

6. Wicked Problems do not Have an Enumerable Set of Potential Solutions, nor is There a Well-Described Set of Permissible Operations that may be Incorporated into the Plan

Whether it is the magnitude of the problem, the time restrictions or simply the ability of the decision makers, this problem does not have an exhaustive list of solutions. Every permutation of the issues will garner different approaches that will have varying degrees of success, but none will completely resolve the dilemma. Further, one commander`s approach to the circumstances may not match approaches taken by his peers, or even his adversaries. Overlay the strategic and political objectives, messages and influences and it is easy to see where new scenarios and potential outcomes further complicate problem resolution.

7. Every Wicked Problem is Unique

How a commander or his adversary uses social media to accomplish his aims today, will be different tomorrow. A political hot topic will only remain in the public eye for a short period of time before the next sound bite or twitter feed is released. The factors faced will change, the message drivers will change, the information will change all requiring unique and new considerations. People move, systems are replaced, analysts reconsider issues, and motivations or opinions shift.

---

[25] Rye Barcott, "The Strategic Corporal." *Harvard Business Review*. **October 2010.** https://hbr.org/2010/10/the-strategic-corporal.html

There will be plenty of good practices proposed to address certain vulnerabilities or risks, but there is no single one-stop-shop for solutions. Installing virus software will not address trend manipulation any more than purchasing more weapons will eliminate non-state actor-driven violence.

8. Every Wicked Problem can be Considered to be a Symptom of Another Problem

The proliferation of social media, its use and protections are symptoms of the greater problem of technology that has outpaced the governance structure of the state and society as a whole. Conflict, in particular, hybrid warfare, has led to state and non-state actors competing for control of the same problem space. Technology has enabled single individuals to access and use the information on the same level as the state, and in some case better and with more flexibility.[26]

9. The Existence of a Discrepancy Representing a Wicked Problem can be explained in Numerous Ways. The Choice of Explanation Determines the Nature of the Problem's Resolution

Within the cyber domain how we frame the problem is extremely important. It is not simply about the need for greater flexibility in social media, or improved protections, or even addressing the mechanisms to collect and analyse intelligence. It is all of this, as they are not just interconnected but they are interdependent to such a degree that there is no one mechanism or border from which to shape resolution. The strategist will tend to focus more on the messaging

[26] Colonel Glenn Voelz and Sarah Soliman. "Identity, Attribution, and the Challenge of Targeting in the Cyberdomain." Marine Corps University Journal Vol.7. No.1 (Spring 2016): 12.

than the risk; the operator will be more concerned with action regardless of the path; the security specialist will tend towards a greater degree of security.

10. The Problem Solver has no Right to be Wrong

Within the cyber domain, the decisions are permanent and everlasting. Once a particular path is chosen and implemented it cannot be reversed or undone. Not only does the decision become permanent, but the ripple effects are wide-ranging and unpredictable. A decision to withhold information prevents a message from reaching all of its potential targets. Lack of action or even just hesitation in implementing protection could affect all systems in a given network, which in itself can propagate to new systems. Messages can be received, but they can also be manipulated as we have seen with fake news stories and trend algorithm tampering.[27] If not controlled these can take on a new life of their own, which can result in a whole new set up problems.

CONCLUSION

The proliferation of data communications, both in terms of physical infrastructure and the applications that operate within it, has played a major role in the globalization of our modern society. While we have become extensively connected through the instantaneous transmission of the messages, human traits remain to influence how those systems are used, and ultimately abused. As we grow more comfortable and in some cases dependent on these systems, the level of potential risks increase both in terms of the frequency and intensity. There is no expectation

[27] Prier, Jarred. "The Command of the Trend: Social Media as a Weapon in the Information Age." Graduate thesis, Air University Maxwell Air Force Base, Alabama, June 2017: 10-30.

that this will end any time soon, which leaves us in the desperate situation where we must develop technologies, protocols, policies and procedures to counter the wide range of threats. With the evolution of social engineering, these protection programs now must be expanded to address the more complex threats that are encountered through widespread use of social media platforms.

With the expansion of Social media comes new and better opportunities within modern operations. The cyber domain is seen by some as its own battlespace. In this context it has all of the elements for both offensive and defensive operations while providing a valuable tool for non-combat efforts such as humanitarian aid, policing and governance. Used effectively it can significantly contribute to kinetic effects, information and intelligence gathering and command and control.

This paper has examined this complex environment of both how we protect our information and how social media has changed the landscape of warfare. It has expanded this evaluation beyond the black and white consideration of Information technology by using Rittel's ten attributes for a wicked problem. This assessment is extremely important, for this problem will continue to grow, and until we truly understand the nature of the problem, we will struggle, and potentially fail to address the many attributes that this consists of.

BIBLIOGRAPHY

Audette-Longo, Trish. "Kinder Morgan Pipeline supporters and Detractors are Being Swarmed by Online 'Bots'." National Observer 20 April 2018. https://www.nationalobserver.com/2018/04/20/analysis/kinder-morgan-pipeline-supporters-and-detractors-are-being-swarmed-online-bots

Barclay, Jack, *Social media growth threatens SF operations.* Jane's Intelligence Review (5 May 2016). https://janes.ihs.com/Janes/Display/jir12142-jir-2016

Barcott, Rye. "The Strategic Corporal." *Harvard Business Review*. October 2010. https://hbr.org/2010/10/the-strategic-corporal.html

Brantly, Aaron F., Nerea M. Cal and Devlin P. Winkelstein. "Defending the Borderland – Ukrainian Military Experiences with IO." *Cyber and EW. Army Cyber Institute at West Point*, 2017.

Canada. Department of National Defence. "National Defence Security Orders and Directives. Chapter 7. Information Technology Security" 11 August 2017.

Canada. Department of National Defence. "National Defence Security Orders and Directives. Chapter 17. Security and Social Media" 15 February 2018.

Canada. Department of National Defence. Photo of Cpl Leclerc on TV Hill Kabul, Afghanistan. Taken by Sgt Frank Hudec, Canadian Forces Combat Camera. 7 May 2004.

Canadian Broadcasting Company. "Canada's Radio Kandahar Goes to Air." CBC News (6 January 2007). http://www.cbc.ca/news/canada/canada-s-radio-kandahar-goes-to-air-1.654396

Collings, Terry. "Trump's Itchy Twitter Thumbs Have Redefined Politics." C-Net 20 January 2018. https://www.cnet.com/news/donald-trump-twitter-redefines-presidency-politics/

Giandomenico, Nena. "What is Spear-phishing? Definition and Differentiating Spear-phishing from Phishing." Digital Guardian 27 June 2016. https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

Herrick, D. *The social* side *of `cyber power'? Social media and cyber operations*. Washington, DC: Piscataway, NJ, 2016.

Horn, R. E. & Weber, R. P. *New tools for resolving wicked problems: Mess mapping and resolution mapping* processes. MacroVU(r), Inc. and Strategy Kinetics, LLC: 2007. http://www.strategykinetics.com/New_Tools_For_Resolving_Wicked_Problems.pdf

Khidzir, N.Z., A.R. Ismail, K.A.M. Daud, M.S.A.A. Ghani, and M.A.H. Ibrahim, *Critical Cybersecurity Risk Factors in* Digital *Social Media: Analysis of Information Security Requirements*. ETPUB - Engineering and Technology Publishing. June 2016, vol.4, no.1, pp. 18-24.

Li Lei and Kai *Qian*. "Using real-time fear appeals to improve social media security." Atlanta, GA USA: IEEE Computer Society, 2016: 610-611. https://ieeexplore.ieee.org/document/7552287/

Prier, Jarred. "The Command of the Trend: Social Media as a Weapon in the Information Age." Graduate thesis, Air University Maxwell Air Force Base, Alabama, June 2017.

Rittel, Horst W.J., and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4, no. 2 (June 1973): 155-169.

Shallcross, Nicholas. "Social Media and Information Operations in the 21st Century" Working Paper, University of Arkansas, February 2016.

Tayouri, David. "The Human Factor in the Social Media Security - Combining Education and Technology to Reduce Social Engineering Risks and Damages." *Procedia Manufacturing* Vol 3 (2015): 1096 – 1100. https://ac.els-cdn.com/S2351978915001821/1-s2.0-S2351978915001821-main.pdf?_tid=6c3250ea-f680-4814-9916-ad924709614b&acdnat=1523685907_6896238ff7ac404a42980385e3de623d

Voelz, Colonel Glenn and Sarah Soliman. "Identity, Attribution, and the Challenge of Targeting in the Cyberdomain." *Marine Corps University Journal* Vol.7. No.1 (Spring 2016): 8-29.

White, Andrew. *Militaries Move to Leverage Benefits of Social Media*. Jane's International Defence Review (18 November 2016). https://janes.ihs.com/Janes/Display/idr18919-idr-2016

White, Andrew. *NATO Centre Draws Up Social Media Exploitation Goals.* Jane's International Defence Review (9 December 2017). https://janes.ihs.com/Janes/Display/FG_696407-IDR

Wright, Teresa "Canadian government spending tens of millions on Facebook Ads, Sponsored Posts." Canadian Press Tues May 22, 2018. https://www.thestar.com/news/canada/2018/05/22/canadian-government-spending-tens-of-millions-on-facebook-ads-sponsored-posts.html