A Model for Characterizing Cyberpower

Adrian Venables, Siraj Ahmed Shaikh, James Shuttleworth

Chapter 1

A MODEL FOR CHARACTERIZING CYBERPOWER

Adrian Venables, Siraj Ahmed Shaikh and James Shuttleworth

Abstract Cyberspace may well be the "great equalizer" where nation states and non-state actors can wield cyberpower and compete on relatively equal terms. Leveraging current views and uses of cyberpower, this chapter redefines cyberspace and introduces a three-dimensional model that expresses how cyberpower can be exercised. The model, which is divided into distinct layers, each with its own unique characteristics, offers a notion of distance through a view of cyberspace that introduces the concepts of near, mid and far space. Cyberpower is examined from the perspective of national security. A range of prominent cyber attacks are qualitatively assessed and compared within the context of the model.

Keywords: Cyberspace, cyberpower, cyber attacks, national security

1. Introduction

This work builds on research by Rowland et al. [18] that describes the anatomy of a cyber power and highlights the essential elements required to achieve and maintain cyberpower. It redefines cyberspace by drawing together and expanding on existing definitions to create a three-dimensional model through which power can be exercised. After deconstructing the notion of cyberpower into a number of constituent components, a range of well-documented examples of cyber attacks are examined within the context of the new model for cyberspace. This provides a foundation for the measurement of cyberpower.

Although power has been defined in a number of ways, this work restricts the definition to national security and conflict, which seek to achieve advantage for political purposes. Thus, the criminally-motivated activities that flourish in cyberspace for financial benefit are excluded as are the social media activities of celebrities and other individuals who seek self-promotion and influence.

As the cyberspace domain is essentially technical in nature, the proposed characterization of cyberpower encompasses several attributes that together

provide a scale of increasing sophistication and capabilities. The ability of an actor to use cyberspace to develop and launch novel, targeted actions that influence the behavior of other persons or devices is considered to be a demonstration of cyberpower. This requires a superior understanding of the nature of cyberspace and ability to precisely maneuver within it. Similarly, acquiring and retaining cyberpower also require an entity to maintain comprehensive situational awareness of its cyberspace assets and to recognize and contain infiltrations and attacks.

2. Related Work

According to Nye [15], power is a contested concept that is elusive to define and measure. Nye also describes the three facets of power. The first is to get others to do what they would not normally do. The second is agenda setting and framing issues in a manner that does not require coercion. The third is the exercise of power by determining the wants of other entities.

Nye also distinguishes hard power from soft power. Whereas conventional hard power changes the behavior of another entity through inducements or threats in the form of economic or military measures, soft power comes from attraction, which includes non-material means such as culture, political values and foreign policy. Nye [14] also develops the notion of smart power where the concepts of hard and soft power are mutually reinforcing. Smart power enables the full range of political, economic and military options to be articulated in a single strategy that advances national policy objectives.

As with the notion of power, arriving at a definitive description of cyberspace is a notoriously difficult task; one study reports 28 different definitions of cyberspace [10]. The Development, Concepts and Doctrine Centre (DCDC) of the U.K. Ministry of Defence acknowledges the lack of a formal definition of cyberspace and, thus, draws on the Concise Oxford English Dictionary definition of cyberspace as relating to "information technology, the Internet and virtual reality." The Joint Doctrine Note 3/13 formally defines cyberspace for the U.K. defense forces as "the interdependent network of information technology infrastructures (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment" [30].

This research views the component elements of cyberspace as a series of layers, with each layer fulfilling a particular role. Initially three layers were considered, the physical layer at the base, a syntactic layer above it and a semantic layer at the top [12]. In this model, the physical layer comprises hardware and cabling, the syntactic layer includes the software and protocols that enable data transfer between the hardware components in the physical layer, and the semantic layer contains the information used by a system to achieve its intended purpose.

Subsequent work developed a four-layer model comprising the infrastructure, physical, syntactic and semantic layers [23]. The infrastructure layer consists of hardware, cabling and satellites; the physical layer incorporates the electro-

Table 1. Three horizontal layers of cyberspace.

Environment	Description
Near Space	Local networks and systems that are considered vital to support the critical national infrastructure and services, and are assumed to be controlled and protected by national or governmental agencies.
Mid Space	Networks and systems that are critical to access global cyberspace, but over which there is no local control or protection. Typically, these assets are geographically distant and are owned by foreign companies or third parties.
Far Space	Networks and systems that form the near space of a competitor or adversary, and must be influenced or controlled as part of a campaign to project power and influence in cyberspace.

magnetic spectrum; and the syntactic and semantic layers retain their original definitions.

In addition to representing cyberspace in terms of layers, cyberspace can be considered geographically in terms of near, mid and far operating space as described in Table 1 and based on the U.K. Ministry of Defence *Cyber Primer* [30]. Control and a comprehensive situational awareness of local near space are vital to protect and defend national and local interests. Power is exerted through the "no man's land" of mid space into far space by traditional power projection mechanisms or cyber attacks; the far space corresponds to the near space of a target country or competitor. An analysis of an adversary's strengths and weaknesses in each of these areas can provide information about the most effective methods that can be utilized to reduce its influence and ability to operate freely in cyberspace.

3. Unified Cyberspace Model

The four-layer model of cyberspace expresses the fact that the ability to control one layer does not imply control of any other layer for the purposes of achieving a specific cyber effect. In fact, all four layers must be considered in a coherent mission planning process.

To fully appreciate the planning required to effectively project power as part of a broader campaign, a unified model has been created that incorporates three new layers and expands the definition of the semantic layer. Figure 1 presents the unified model, which comprises seven layers from bottom to top: (i) services layer; (ii) infrastructure layer; (iii) physical layer; (iv) syntactic layer; (v) semantic layer; (vi) human layer; and (vii) mission layer.

The services layer lies below the infrastructure layer and emphasizes the dependencies between components of the infrastructure layer that enable cyberspace to exist and function. It includes resources such as power, water,

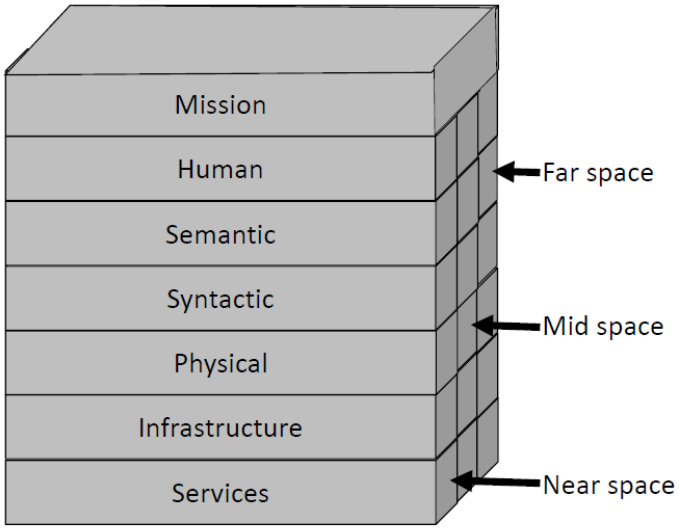

Figure 1. Unified cyberspace model.

materials and even physical security. This layer also includes industrial systems and components that support the infrastructure.

Cyberspace requires human intervention for its creation, maintenance, exploitation and (even) its destruction. Thus, a human layer is included directly above the semantic layer. The semantic layer, which provides information that is useful and understandable to human operators, is necessarily expanded to cover the specific needs of end users. This includes language, culture and user interactions in cyberspace. The importance of this aspect of communicating information is recognized in the field of social network analysis, which investigates the characteristics of relational ties to draw inferences about a network and its entities [22].

The mission layer is the capstone of the unified cyberspace model. It emphasizes the fact that cyberspace serves human needs that are constantly evolving and expanding, and that cyberspace is not a naturally-occurring phenomenon. Every interaction in cyberspace has a specific purpose and consequence, whether intentional or unintentional, innocent or malevolent. By specifying and highlighting the notion of a mission at the top of the model, the roles of all the lower layers can be better understood and contextualized.

Upon combining the seven layers of cyberspace with the concepts of near, mid and far space, cyberspace can be redefined in terms of the three dimensions shown in Figure 1. This can be used to further illustrate that, although cyberpower may be exercised in some elements of cyberspace, it does not guarantee control of all the elements and that a technique that targets a particular aspect may only have a limited overall effect against an adversary. This model also enables attacks to be appreciated in terms of their intended effects and

where the greatest risks to an organization exist. It should also be noted that, because the mission element does not vary from mid to far space, it remains a constant throughout.

4. Defining Cyberpower

This section defines the notion of cyberpower and distinguishes between state and non-state actors.

4.1 Cyberpower

Cyberpower may be defined as the ability to alter the behavior of a target subject through the medium of cyberspace in the context of national security and conflict. Such power is exercised by state or non-state actors via cyber campaigns that comprise a singular targeted event (or series of events) using coercive, persuasive or technical means to achieve a specific effect as part of a strategic objective. This ability can be broken down into the following distinct capabilities:

- Active engagement and influence aimed at understanding and opinion forming with a view to directing policy and discourse in the cyber domain using the projection of soft power.
- Targeted and possibly offensive measures designed to deny, degrade, destroy, disrupt or divert service or data to particular devices or components to achieve specific objectives.
- Resilience of the cyber infrastructure through the effective anticipation, absorption, adaptation and recovery from a cyber campaign. A cyber campaign can consist of hard, soft or smart power techniques available to a state or non-state actor and may be realized via a combination of technical and policy mechanisms to strengthen, adapt and defend the infrastructure. This is achieved through reconnaissance and intelligence to maintain a comprehensive situational awareness of assets located in near space.
- Resources and means to achieve attribution of the full spectrum of cyber campaigns in order to counter and, if necessary, take retaliatory action.
- Technical skills and the capacity to underpin the effective and sustained delivery of all of the above.

4.2 State and Non-State Actors

Cyberspace can be regarded as the "great equalizer" in which nation states and non-state actors can compete on relatively equal terms. It can offer entities the same speed, reach, anonymity and protection as well as the ability to develop their own cyber weapons at low cost while profiting economically from

on-line commerce [19]. The differences between state and non-state actors are highlighted by comparing their published cyber strategies or previously-demonstrated offensive activities in cyberspace to determine where their priorities lie and where they reside in the unified model of cyberspace.

Several countries have published their national cyber strategies. The United Kingdom and the United States emphasize their increasing dependence on cyberspace and the risks that this brings, noting the dichotomy between the need to tackle security threats while respecting privacy and other fundamental rights. The 2011 United Kingdom Cyber Security Strategy [29] presents a vision to derive economic and social value from cyberspace and emphasizes the economic benefits as well as the need to tackle cyber crime and be resilient to cyber attacks. The human aspect of security is also recognized with the need to develop the knowledge, skills and capabilities required to meet the overall security objectives.

The United States recognized the need for a policy to secure cyberspace as far back as 2003 with the publication of a national strategy [3]. This strategy articulated a framework for protecting the infrastructure that is essential to the economy, security and way of life. The 2011 United States Department of Defense's strategy for operating in cyberspace is predominantly defensive in nature and treats cyberspace as an operational domain [31]. In particular, the strategy covers the protection of Department of Defense networks and systems using the skills of its workforce and through partnerships with other departments and allies. The theme of international cooperation is also the subject of the 2011 U.S. International Strategy for Cyberspace [16]. One of the important goals is to work with the international community to promote an open, interoperable, secure and reliable information and communications infrastructure [16].

The need for international collaboration to secure cyberspace is also recognized by NATO in its National Cyber Security Framework Manual [8]. The manual notes that, although national interests tend to have priority over common interests, international cooperation is needed to achieve cyber security at the global level. The NATO Cooperative Cyber Defense Center of Excellence (CCDOE) has identified international laws that are applicable to cyber warfare in its Tallinn Manual [20]. Released in 2013, the manual specifies 95 rules governing cyber conflicts, addressing issues such as sovereignty, state responsibility, international humanitarian law and the law of neutrality. The European Commission has also recognized the need to achieve an open, safe and secure cyberspace, which it seeks to achieve through its norms and principles of fundamental rights, democracy and the rule of law [4].

Although several nation states have published their official (defensive) cyber policies, they tend to be very reticent about exposing details of their offensive doctrines or capabilities. However, this is not the case with some non-state actors who have amply demonstrated their intent and capabilities to conduct a wide spectrum of cyber attacks [5]. The Anonymous collective is the most prominent western non-state group and it has demonstrated significant cyberpower. The collective, which first came to prominence after its attacks on the

Church of Scientology in 2008, achieved significant publicity with a campaign of action in support of Wikileaks against PayPal and the hacking of the security firm HBGary in 2011 [24]. Anonymous is difficult to quantify because it claims to be a leaderless collective operating under the mantra: "Knowledge is free. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us." Its significant social media presence grants it status as a cyber power according to the definition given above, especially when considering the sophistication of its activities (e.g., support of Wikileaks) [21].

The Syrian Electronic Army is a formidable group that has supported the government of Syrian President Bashar al-Assad. Although its relationship with the government is unclear and despite its claims to be independent, some commentators speculate that the Syrian Electronic Army is a state-sponsored entity [17]. State sponsored or not, the group is well organized with its own website, which lists its high profile hacks, including successful attacks on the western media and the U.S. Marine Corps website [28].

In general, nation states publish their cyberspace strategies and emphasize the need for resilience. This concentrates their efforts on the protection of near space for reasons of economic and national security. Non-state actors, however, typically operate in mid space and do not have the burden of protecting their infrastructures in near space. Instead, their activities are limited to exerting cyberpower in the near space of their adversaries according to their political and conflict agendas. This enables non-state actors to maintain resilience through distribution and anonymity, although their capabilities may not be focused and sustained because they primarily rely on volunteers to pursue their agendas. The key difference between nation states and non-state actors is that the former are constrained by domestic and international law, while the latter consider themselves free to use any and all means that are deemed to be effective.

5. Characterizing Cyberpower

This section characterizes cyber attacks, and by extension cyberpower, in terms of six attributes that are used to provide a composite score of the sophistication of a cyber campaign. Also, the section evaluates ten well-publicized cyber attacks from 2007 through 2014 with respect to the six attributes and provides the corresponding composite scores.

5.1 Cyber Attack Attributes

Having defined the concepts of cyberspace and cyberpower in the context of the unified model, it is possible to characterize the effects of cyber attacks and to measure cyber attacks and, by extension, cyberpower. Cyber attacks are measured using a sophistication scale based on the layers in the cyberspace model, which combined with the targeted activities, provides a comparative scaling of the attacks. Sophistication is measured in terms of six characteristics, persistence, propagation, novelty, precision and accuracy, impact and attribution:

- **Persistence:** This is measured in terms of the actions or effort undertaken by the attacker. For example, a denial-of-service attack requiring continued action from an attacker would score less than a virus that does not require human action to propagate. Accordingly, a virus would score less than a self-replicating worm that requires no originator interaction after the initial delivery.

- **Propagation:** This is measured in terms of the effort that is required to deliver the payload. For example, a successful attack on a system that is not connected to the Internet would score higher than a system that is more easily accessed.

- **Novelty:** This is measured in terms of the uniqueness of the technique employed by the attack payload and the amount of effort expended in its development. The use of previously-unknown exploits would receive a high score.

- **Precision and Accuracy:** These are measured in terms of how discreet the attack is in achieving a particular effect. This considers the level of collateral damage to other systems or people and the extent to which the timing of the event can be determined. An attack that focuses on a unique target at a specific time would score more highly than a general widespread attack with no particular timing because it indicates the complexity of the objective or a desire to reduce collateral damage.

- **Impact:** This is measured in terms of the effectiveness of the attack, which depends on its psychological value as well as the actual effect on the target. Impact can also be measured in terms of the temporal effect. The scoring is influenced by the publicity and assessment of cyber security researchers who identify precise attack details that have not been released to the public. The more severe the impact, the higher the score.

- **Attribution:** This is measured in terms of the ability of the target of a cyberpower campaign to accurately identify the originator. The originator may seek total anonymity or may imply that another group or country executed the attack in order to hinder the investigation. The scoring index depends on the mission of the cyber attack; although, in general, the greater the anonymity, the higher the score.

5.2 Cyber Attack Evaluation

Tables 2 and 3 describe ten significant cyber attacks from 2007 through 2014. The attacks are characterized in terms of near, mid and far space, and the layers of the unified cyberspace model in which they were active. Numerous attacks have been publicized, but these ten attacks were selected due to their relevance to the definition of cyberpower as being related to national security

Table 2. Characterization of cyber attacks.

Attack	Attack Details and Degree of Sophistication
DDoS (2007) [9]	Coordinated distributed denial-of-service attack on Estonia's infrastructure through near, mid and far space. The attack, although large in scale, used relatively unsophisticated methods and was launched over the Internet. Although it generated considerable publicity, it was relatively short-lived with limited long-term damage. Active Layer: Syntactic. Persistence, Propagation, Novelty, Precision, Attribution: Low; Impact: Medium. *Total Score = 7.*
Aurora (2009) [25]	Targeted malware attack against Adobe and Google through near, mid and far space. The attack, thought to be state-sponsored, targeted at least 30 companies and employed a previously unknown Internet Explorer vulnerability that enabled computers to be controlled and data to be exfiltrated [7]. The attack was eventually neutralized by browser and anti-virus updates. Active Layer: Semantic. Propagation, Precision: Low; Persistence, Novelty, Impact, Attribution: Medium. *Total Score = 10.*
Stuxnet (2010) [27]	Highly-sophisticated malware thought to be state-sponsored and believed to have targeted an industrial control system in far space that could not be directly accessed via the Internet. The malware used an unprecedented number of previously-unknown Microsoft vulnerabilities and also compromised the human-machine interfaces of the control system. Active Layers: Services, Infrastructure. Persistence, Propagation, Novelty, Precision, Impact, Attribution: High. *Total Score = 18.*
Duqu (2011) [1]	Stuxnet-like malware that targeted the Microsoft Windows operating system to steal information located in far space. The malware sought information about industrial control systems and exfiltrated the information through mid space to the originator's near space. Active layer: Syntactic. Propagation, Precision, Impact, Attribution: Medium; Persistence, Novelty: High. *Total Score = 14.*
HBGary (2011) [24]	Attack attributed to Anonymous. This relatively-unsophisticated attack against HBGary through mid and far space exploited known vulnerabilities to exfiltrate sensitive data and conduct a denial-of-service attack. Active Layers: Semantic, Human. Propagation, Novelty, Attribution: Low; Persistence: Medium; Precision, Impact: High. *Total Score = 11.*

or conflict. Additionally, the attacks were selected because substantial open source information was available for analysis.

Table 3. Characterization of cyber attacks (contd.).

Attack	Attack Details and Degree of Sophistication
Flamer (2012) [26]	Malware with a complexity similar to Stuxnet and Duqu, albeit unrelated. Thought to be state-sponsored, the malware targeted Eastern Europe and Middle Eastern countries to exfiltrate information from a range of targets in far space through mid space to near space. Active Layer: Syntactic. Precision: Low; Propagation, Impact, Attribution: Medium; Persistence, Novelty: High. *Total Score = 13.*
Shamoon (2013) [2]	Highly targeted and widespread attack in far space on the critical infrastructure of Saudi Aramco by means of a self-replicating virus that deleted data and rendered computers unusable. Thought to be state-sponsored. Active Layer: Infrastructure. Propagation: Low; Persistence, Novelty, Precision, Impact, Attribution: High. *Total Score = 16.*
APT1 (2013) [13]	Widespread industrial espionage of western commercial enterprises in far space using complex and well-organized procedures with evidence of state-sponsorship in near space. Active Layer: Semantic. Propagation: Low; Persistence, Novelty, Precision, Impact, Attribution: Medium. *Total Score = 11.*
ISIL (2014) [6]	Non-state sponsored campaign through social media in mid space targeting domestic and western media using high production quality media to publicize activities, attract and encourage supporters and intimidate adversaries. Active Layers: Semantic, Human. Propagation, Precision, Attribution: Low; Persistence, Novelty: Medium; Impact: High. *Total Score = 10.*
Sony (2014) [11]	Possible state-sponsored attack on Sony Corporation that resulted in the exfiltration and publication of sensitive information in far space causing embarrassment and financial loss. Active Layers: Semantic, Human. Persistence, Propagation: Low; Novelty, Attribution: Medium; Precision, Impact: High. *Total Score = 12.*

The grades, low, medium and high, correspond to the numerical scores, 1, 2 and 3, respectively. The numerical scores assigned to the individual characteristics were added to yield the total score. The grades and, thus, the scores were qualitatively assessed based on expert opinion. Note that all the characteristics were given the same weight, although, in some circumstances, certain criteria may necessitate higher relative values.

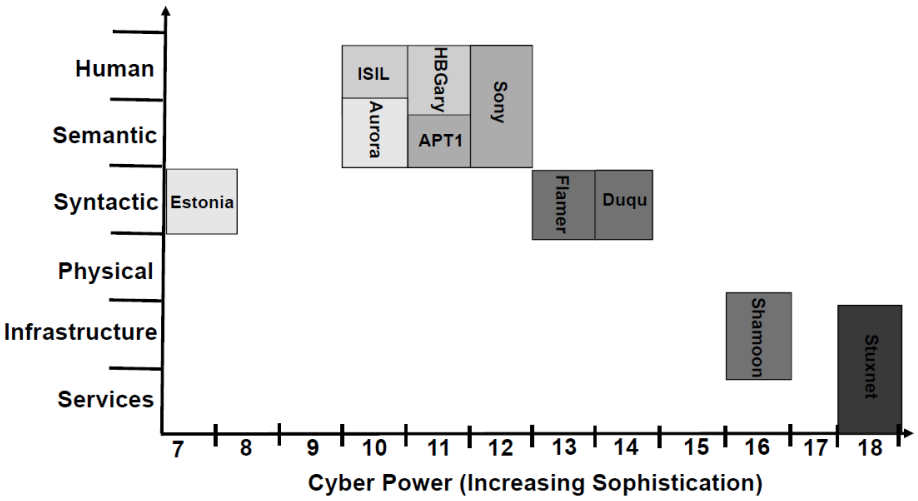

Figure 2. Comparison of cyber attack sophistication and layers of operation.

Figure 2 displays the information provided in Tables 2 and 3 in a graphical format, indicating the relative sophistication of the attacks and the layers of cyberspace in which they were active. The figure shows a general trend that indicates a less complex and less technically-challenging approach is adequate to attack the semantic and human layers. This is because these layers are designed to be readily accessible and, therefore, require less effort to achieve successful interactions. The human targets are not only easier to access, but are also more susceptible to influence and change than programmed technical components, which only have a limited series of responses to the possible inputs.

Creating effects in the layers that are not designed for direct human interaction (e.g., services, infrastructure, physical and syntactic layers) are more complex undertakings. This is because an attack involves creating an effect contrary to that envisioned by the system designers and, consequently, requires a deeper understanding of the system architecture and configuration. In addition, an attack conducted over a network that is designed to cause physical damage to a specific system has to be carefully targeted and calibrated to reduce collateral damage.

If it is determined that a physical effect is desired on a system and that impacting the lower elements of a network would require considerable preparation and planning, an alternative strategy may be more effective. Depending on the circumstances, it may be decided that the most timely, economical and effective way of achieving the desired effect is to attack the target using conventional munitions instead of a cyber attack. However, a decision that weighs the strengths and weaknesses of the different options can only be made after a thorough analysis of the target, which can be aided using the unified model of cyberspace and the measures of attack sophistication discussed above.

From the perspective of a cyber attacker, influencing a target at the semantic and human layers tends to require the least sophisticated methods (e.g., an attack via social media). However, the level of complexity required to influence the lower levels and ultimately attack the infrastructure or connected services or systems to achieve a physical effect is much greater. In general, only nation states have the level of sophistication required for complex covert data exfiltration or attacks on the services and infrastructure layers; non-state actors are limited to less sophisticated attacks or relatively overt data extraction. Nevertheless, the asymmetrical nature of these operations is an important factor in strategic offensive and defensive planning.

6. Conclusions

The division of cyberspace into near space, mid space and far space presents an opportunity to maintain cyber situational awareness and enable counter attacks. This contributes to resilience via the anticipation, absorption, adaptation and recovery from attacks, which is an important factor in establishing cyberpower. The specification of what constitutes near space enables the articulation of defensive priorities and the identification of far space boundaries that lower the risk of incurring collateral damage. Combining situational awareness with the quantification of the various layers of cyberspace can improve the understanding of cyberspace and how to project cyberpower.

Future research will attempt to further delineate the elements of cyberspace and quantify cyber attacks and the cyberpower of nation states and non-state actors. The goal is to develop a model that can provide numerical indices of cyberspace and cyberpower, and assist with the prediction of attack effectiveness. Such a model would significantly inform defense policy and spending priorities. Clearly, reliable data sources will be required to develop and validate the model. Future research will also evaluate government and industry databases to determine what information is already available and what information remains to be collected.

References

[1] B. Bencsath, G. Pek, L. Buttyan and M. Felegyhazi, Duqu: A Stuxnet-like Malware Found in the Wild, Technical Report, Laboratory of Cryptography and System Security, Department of Telecommunications, Budapest University of Technology and Communications, Budapest, Hungary ((`www.crysys.hu/publications/files/bencsathPBF11duqu.pdf`), 2011.

[2] C. Bronk, The cyber attack on Saudi Aramco, *Survival: Global Politics and Strategy*, vol. 55(2), pp. 81–96, 2013.

[3] G. Bush, National Strategy to Secure Cyberspace, The White House, Washington, DC, 2003.

[4] European Commission, 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 the Regions, JOIN(2013) 1 Final, Brussels, Belgium, 2013.

[5] European Union Agency for Network and Information Security (ENISA), National Cyber Security Strategies in the World, Heraklion, Greece, 2014.

[6] F. Irshaid, How ISIS is spreading its message online, *BBC News*, June 19, 2014.

[7] A. Kliarsky, Responding to Zero Day Threats, InfoSec Reading Room, SANS Institute, Bethesda, Maryland (`www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709`), 2011.

[8] A. Klimburg (Ed.), National Cyber Security Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia (`www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf`), 2012.

[9] A. Kozlowski, Comparative analysis of the cyber attacks on Estonia, Georgia and Kyrgyzstan, *European Scientific Journal*, vol. 3, pp. 237–245, 2014.

[10] F. Kramer, Cyberpower and national security: Policy recommendations for a strategic framework, in *Cyberpower and National Security*, F. Kramer, S. Starr and L. Wentz (Eds.), National Defense University Press and Potomac Books, Washington, DC, pp. 3–23, 2009.

[11] T. Lee, The Sony hack: How it happened, who is responsible, and what we've learned, *Vox*, December 17, 2014.

[12] M. Libicki, *Cyberdeterrence and Cyberwar*, RAND, Santa Monica, California, 2009.

[13] Mandiant, APT1: Exposing One of China's Cyber Espionage Units, Mandiant Intelligence Center Report, Alexandria, Virginia (`intelreport.mandiant.com`), 2013.

[14] J. Nye, *Soft Power: The Means to Success in World Politics*, PublicAffairs, New York, 2004.

[15] J. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University, Cambridge, Massachusetts, 2010.

[16] B. Obama, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, The White House, Washington, DC, 2011.

[17] N. Perlroth, Hunting for Syrian hackers' chain of command, *New York Times*, May 17, 2013.

[18] J. Rowland, M. Rice and S. Shenoi, The anatomy of a cyber power, *International Journal of Critical Infrastructure Protection*, vol. 7(1), pp. 3–11, 2014.

[19] J. Rowland, M. Rice and S. Shenoi, Whither cyberpower? *International Journal of Critical Infrastructure Protection*, vol. 7(2), pp. 124–137, 2014.

[20] M. Schmitt (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, United Kingdom, 2013.

[21] M. Schwartz, Who is Anonymous: 10 key facts, *Information Week – Dark Reading*, February 6, 2012.

[22] J. Scott and P. Carrington (Eds.), *The SAGE Handbook of Social Network Analysis*, Sage Publications, London, United Kingdom, 2011.

[23] J. Sheldon, Deciphering cyberpower: Strategic purpose in peace and war, *Strategic Studies Quarterly*, vol. 5(2), pp. 95–112, 2011.

[24] P. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York, 2014.

[25] Sophos, Operation Aurora: What you need to know, Abingdon, United Kingdom (`www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx`), 2010.

[26] Symantec, Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East, Mountain View, California (`www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east`), 2012.

[27] Symantec, W32.Stuxnet, Mountain View, California (`www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99`), 2013.

[28] Syrian Electronic Army, Syrian Electronic Army Homepage (`www.sea.sy`), 2015.

[29] U.K. Cabinet Office, The U.K. Cyber Security Strategy: Protecting and Promoting the U.K. in a Digital World, London, United Kingdom (`www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf`), 2011.

[30] U.K. Ministry of Defence, Cyber Primer, Development, Concepts and Doctrine Centre, Shrivenham, United Kingdom, 2013.

[31] U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace, Washington, DC, 2011.