Victory in Cyberspace

Miguel Alberto Gomez, Center for Security Studies, ETH Zurich, Switzerland

The Asia-Pacific Conference on Security and International Relations 2016
Official Conference Proceedings

Abstract
A review of state-initiated and state-sponsored incidents in cyberspace over the past decade reveals that over two thirds of these involved actors within the Asia-Pacific, often occurring in the context of politico-economic disputes. These activities, ranging from attempts at espionage to coercion, in all appearance appears to confirm the domain's increasing strategic value. But upon closer inspection, only half of these have resulted in meeting their political objectives. Moreover, these have involved notable regional powers employing relatively unsophisticated tools and tactics in cyberspace. This challenges the prevailing notion that cyberspace provides an asymmetric advantage for middling and/or weak powers due to its low cost of entry and the increasing technological dependence of targets. With growing tensions in the Asia-Pacific, the need to better understand the strategic utilization of this domain is paramount. In so doing, this paper argues that coercive success in cyberspace is not determined solely by an aggressor's technological prowess but depends crucially on appropriate force employment and an understanding of the domain's unique geography. Through the analysis of the Stuxnet operation, the paper demonstrates that careful consideration of these factors may better account for the success or failure of coercion in the domain.

Keywords:Cyberspace, Strategy, Coercion

Cyberspace and Failed Promises

The appearance of state-initiated or state-sponsored cases of cyber operations in conjunction with disputes in the physical domain has become commonplace over the past decade. As heralded by Arquilla and Ronfeldt's prescient article back in 1994, the perceived strategic utility of cyberspace has encouraged state actors to employ it as a coercive tool aimed at shifting an adversary's behavior in their favor (Arquilla & Ronfeldt, 1993). Prominent cases such as the Estonian Distributed Denial-of-Service (DDoS) in 2007 and the discovery of Stuxnet aimed at Iranian nuclear centrifuges in 2010 have buoyed initial claims of the advantages provided by operations in cyberspace. Moreover, these cases support the prevailing notion of a "cyber revolution" that will (or has) changed how states pursue their foreign policy objectives.

On the one hand, while cyber operations are indeed on the rise, they have proven to be far less effective than originally conceived. For instance, coercive cyber operations have succeeded less than three-percent (3%) of the time (Valeriano & Maness, 2014). Furthermore, despite increased dependence on cyberspace in support of political, economic, and military objectives, advanced cyber operations that could pose a threat to these have failed to inflict lasting damage capable of altering the balance of power. The paradox that exists between the dominant "cyber revolution" thesis and that of the empirical evidence calls for further investigation of the causal dynamics that lead to the successful use of coercive cyber operations.

While several factors exist that influence the outcome of coercion (Pape, 1996; Schelling, 2008), this paper narrows its focus on the unique characteristics of cyberspace and on variations of actor perceptions towards the domain and how it contributes to success or failure of coercion. This view stands in contrast with the propositions of an on-going "cyber revolution" that espouse a monolithic and uniform view of the domain. To demonstrate the feasibility of this alternative account, a representative case is selected and analyzed using the proposed framework. The objective of which is not to discredit previous arguments that support the predominant view, but rather, to offer a theoretically grounded argument to account for events in this domain.

In so doing the paper proceeds as follows. The succeeding section offers a brief overview of the concept of coercion as it applies to the traditional domains of air, sea, and land. This sets the tone of the next which presents how the "cyber revolution" thesis fits with the unique geography of cyberspace. Furthermore, this section walks the reader through the logic of coercion in cyberspace rooted in prevailing framework. After which, the paper presents an alternative account centered on perceptive differences with regards to the importance of cyberspace as a key factor for the success of coercive operations. It is in this section that the paper's primary arguments are presented. Following this, the methodology used is presented that allows for the case in the following section to be analyzed using both the "cyber revolution" thesis

and the alternative proposed herein. Finally, the paper concludes with a discussion of the initial results and the possible direction that later inquiries may take.

Coercion: A Recap

The use of coercive operation to attain the strategic interests of a state has a long, and perhaps dubious, history that stretches far back in history and well into the modern era. Commonly seen as the "power to hurt", coercion is the use or threat of force aimed at changing an adversary's behavior (Schelling, 2008). Crucial in the exercise of such is the ability to force an adversary to re-assess the cost of non-compliance versus the benefits of yielding to coercive demands.

Although the exact terminologies concerning coercion is still open to debate, these activities are classified into two general categories depending on the point in time when they are exercised: deterrence or compellence. Deterrence is enacted prior to an adversary engaging in an action that is viewed as unfavorable by the coercer. As such, deterrence attempts to prevent a change in the status-quo by threatening costs should an adversary deviate from their current behavior. In some sense, this may present deterrence as less costly and easier to attain as an adversary has little to no sunk costs involved and is primarily concerned with costs emerging from non-compliance and the loss of future benefits. In contrast, compellence aims to alter the current behavior of an adversary and is reactive rather than preventive. Unlike deterrence, changing an on-going behavior is thought to incur more costs as an adversary would not only have to worry about foregoing future benefits but also the resources that have been employed to reach this point. Furthermore, the potential cost of non-compliance needs to be assessed as well. Consequently, compellence is thought to be more difficult than deterrence (Schaub, 2004; Schelling, 2008).

Apart from timing, coercion is also differentiated based on its intended recipient(s) and may manifest as denial or punishment strategies (Pape, 1996). The former refers to inflicting or threatening costs to prevent an adversary from attaining their political or strategic objectives. This entails targeting assets or infrastructure critical to these objectives. In contrast, punishment strategies aim to increase the cost and/or risk to the civilian population by targeting them directly in the hopes of putting pressure on the government at the time. The former is exemplified by the targeted bombing of German industries during World War II while the latter is typified by the fire-bombing of Japanese cities during the same period.

Even though coercion is usually exercised in the physical domain, similar actions have taken place in cyberspace over the past decade. Yet regardless of its man-made nature, coercion through this virtual domain operates with the same premises albeit adapted to the domain's unique characteristics. The succeeding section furthers this argument and links the unique geography of this domain to the prevailing "cyber revolution" thesis that predicts coercive success.

Geography, Interdependence, and Coercion

In lieu of the abstracted nature through which most interact with cyberspace, it is reasonable that most treat the domain as a monolithic and featureless space. While this may have arisen from the need to provide an abstraction to enable its efficient use, this is not the actual case (Hansen & Nissenbaum, 2009). While a consensus on the true nature of cyberspace remains elusive, the components that form the unique geography of the domain may be divided into three (3) primary layers: Physical, Syntactic, and Semantic (see Figure 1) (Libicki, 2010).

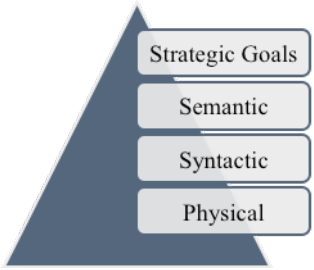

Figure 1 Layers of Cyberspace

The Physical layer refers to the underlying infrastructure that support the generation, transmission, and storage of electro-magnetic signals (e.g. servers, cables, computers, etc.). In contrast, the Syntactic layer is comprised of codes and protocols that allow for the proper construction, manipulation, and transportation data. Despite the popular notion that cyberspace exists independently of the physical domain, it is only at this layer that such a notion is validated. Finally, the Semantic layer allows for the transformation of the data into meaningful information that may be used to support human endeavors (e.g. retail, communication, etc.) (Libicki, 2010). The conversion of electro-magnetic signals into data that is then interpreted into useful information forms the construct that is cyberspace and is thought to be increasingly significant to not only individuals but states as well in support of their strategic interests. As observed by Starr, cyberspace is increasingly becoming an enabler for instruments of national power (Starr, 2009). It is through this logic of interdependency that the coercive potential of cyberspace begins to take shape.

Despite efforts to secure this domain from threats against its confidentiality, integrity, and availability it is thought to be continually at risk. Compounding this challenge is its underlying complexity that demands specialized knowledge to manage and has cultivated an image that portrays cyberspace as being both vulnerable and unknowable with the potential of inadvertent disaster (Hansen & Nissenbaum, 2009). The perceived vulnerability stems from the interdependent and interconnected operation of its underlying components that increases the possibility of flaws to be introduced into the design process. Furthermore, its complexity presents further constraints in addressing these vulnerabilities to the extent that completely mitigating these is highly unlikely. This inability to identify and remedy each and every issue introduces a sense of inevitability such that should an adversary be able to identify an overlooked vulnerability, the domain itself is open to compromise (Dunn-Cavelty, 2013).

These factors that may result in disaster are enablers of the "cyber revolution" thesis. As states increasingly become dependent on cyberspace for their strategic interests, its vulnerable and unknowable nature may lead to an inevitable compromise that allows an aggressor to threaten or inflict costs, possibly threatening strategic interests (Dunn-Cavelty, 2013; Gandhi et al., 2011). Furthermore, the coercive potential of cyber operations is enhanced by the offensive advantage that is thought to exist within cyberspace (Saltzman, 2013).

Plainly stated, an offensive advantage signals a shift in favor of offensive actions relative to defensive ones. Such imbalances have often followed the emergence of new military technologies that provide aggressors a key advantage over defenders. In cyberspace, this advantage is manifested in both the mobility and damage potential of cyber operations because of the interdependence that exists between the different layers of the domain and between cyberspace and a state's strategic interests. Mobility refers to the ability of an operation to impact the different layers of the domain. The effects of an operation against the Syntactic later, for instance, can percolate up to the Semantic layer which ultimately influences strategic capabilities (Saltzman, 2013). Similarly, the damage potential of cyber operations follows a similar logic. Damage inflicted at the lower levels can rise to higher levels and increases in severity as it rises (see Figure 2). To provide an example of this process, consider the case of State A and State B.

If State A is heavily dependent on its economic prowess to further its interests, and given that its economy is supported by a digitized banking system, then attempts to coerce State A may involve threats against its economic infrastructure. To this end, State B can launch an operations that manipulate or delete information stored in its servers thus targeting the Syntactic layer. The loss of information limits its ability to conduct financial transactions at the Semantic layer. If the situation is not rectified and persists, this economic disruption may translate into long term consequences that may affect State A's strategic interests – to the benefit of State B.

Figure 2 Coercive Potential

The example presented above surfaces the key propositions that support the success of coercive cyber operations based on the logic established by "cyber revolution" thesis. First, *the likelihood of coercive success increases if cyber operations exhibit a high degree of mobility*. Second, *the likelihood of coercive success increases if cyber operations are capable of inflicting significant damage*.

Unfortunately, this logic of threatening or inflicting costs against an adversary's strategic interests through cyberspace has not borne much success despite the exercise

of advanced capabilities that meet the above requirements. Estonia in 2007, for instance, is highly dependent on cyberspace to support its economic and political interests experienced an operation aimed at these components that lasted for over two (2) weeks. Despite a lack of precedence, the massive DDoS attack did not lead to any behavioral changes on the part of the target. Similarly, the operation against Iran's nuclear centrifuges that saw the first case of a "weaponized" malware only led them to harden their resolve and develop their own cyber capabilities in turn (Healey, 2016). Interestingly, cases with outcomes diverged from the above predictions challenge the assumptions grounded on the "cyber revolution" thesis. Thusly, the empirical evidence calls into question the suitability of the preexisting theory as it stands and encourages an alternative account for the success of coercive cyber operations.

Vulnerability and Perspective

While the empirical evidence does indeed indicate increased dependence on cyberspace in conjunction with the continued presence of exploitable vulnerabilities, the limitations of existing explanations for coercive success rests on a generic perception of the domain. While the mechanism described by the "cyber revolution" thesis is logically sound, its assumption that cyberspace is valued uniformly across states is unfounded. In the context of coercion, understanding the value placed on certain assets relative to their strategic importance is crucial for success. As noted by Pape, the successful application of coercive threats or action rests on the ability to discern the vulnerabilities of a target such that its execution hinders an adversary's ability to meet its political and/or military objectives (Pape, 1996). This suggests that an aggressor must have knowledge of how an adversary values certain assets in its possession.

With respect to cyberspace, little has been said with respect to variations in the perception of the domain. These differences, however, are apparent in definitions of cyberspace across states. Russia, for instance, views it as the "*area of activity related to the formation, creation, transformation, transmission, use and storage of the information affecting...the individual and social consciousness...*" (NATO CCDCOE, 2016). In contrast, the United States treats it as "*a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data...*" (NATO CCDCOE, 2016). Although similarities exist between the two – notably the emphasis on technology – a key difference lies in the fact that the former endows it with a degree of social significance. Variations such as these suggest not only differing views as to the nature of the domain, but possibly an incompatible valuation of the domain.

To account for the emergence of these differences, Hare initially applied Buzan's model to map state characteristics against possible threats to cyberspace. Initially, the model takes into consideration (military) power (P) and socio-political cohesion (SPC) as key determinants. Hare argues that states with high levels of SPC are generally affected by cyber operations aimed at the Syntactic and Semantic layers –

with an emphasis on the former. This is due to the dependence of such states on cyberspace for economic stability and communication. In contrast, those with low levels of SPC, are consistently vulnerable to de-stabilizing political actions which are associated primarily with the Semantic layer and the manipulation of information. The role of power in these cases is to broaden or narrow the range of vulnerabilities expected to include those that may not directly impact the interest of the state (i.e. private individuals) (Hare, 2010).

Socio-Political Cohesion	CSO	Vulnerability	Primary Affected Layer
High	Positive	Attacks against critical infrastructure	Syntactic
Low	Negative	Destabilizing political action	Semantic

Table 1 Objectives and Vulnerabilities

Hare's model is later simplified by Rivera who omits the dimension of power and relates state vulnerabilities to specific objectives with respect to cyberspace. In his paper, Rivera argues that states can be classified based on their respective Cyberspace Security Objectives or CSOs. These represent the goals of states in securing cyberspace to enable it to meet their strategic interests. States with Positive CSOs (P-CSO) conduct actions that treat cyberspace as a domain for liberal democratic values. Essentially, this entails ensuring availability of information and open discourse, enabling commerce through the domain, and combating crime. Inversely, those with Negative CSOs (N-CSO) engage in actions that limit that restrict the flow of information to ensure that the interests and stability of the regime is not threatened by activities in cyberspace. State initiatives such as censorship, policing social-media, and the like are representative of such (Rivera, 2015). With respect to both types, disrupting these objectives or threatening their successful implementation may negatively impact the strategic interests of states. Consequently, this meets the requirements of coercive success as previously mentioned.

The arguments presented in this section point to two critical differences with respect to the "cyber revolution" thesis in terms of successful coercive cyber operations. First, while states are indeed increasingly becoming more dependent on the domain, *the success of coercion rests on threatening the appropriate CSO of an adversary*. Second, while identifying the appropriate CSO is indeed crucial, each type is reliant on a specific layer of cyberspace. Consequently, *the success of coercion rests on operations that impact the significant layer of cyberspace relative to the CSO*.

With these propositions, two competing accounts for the outcome of coercion in cyberspace are surfaced. On the one hand, coercion may be achieved using advanced capabilities that exploit the unpredictable yet interdependent nature of cyberspace. On the other, success is a function of correctly acknowledging how the domain is valued by an adversary and exercising threats or force accordingly.

Design, Operationalization, Selection

Although support for the alternative account presented herein would be best served by generalizing its findings across all cases of coercion of cyberspace, the lack of data to allow for a large-n study continues to plague research in cyberspace. Consequently, the paper adopts a design based on a representative case to illustrate the applicability of the "cyber revolution" thesis and to demonstrate the ability of alternative explanations to better explain the outcome of coercive activity in cyberspace. At this point it is crucial to mention that the results presented are not definitive, but rather, serve to demonstrate the applicability of this line of reasoning. In so doing, the paper opens a new line of inquiry by offering a starting point for future scholars.

Apart from the overall design, the operationalization of the independent and dependent variables are equally significant. There is no generally accepted measure for either Mobility or Damage Potential. However, specific operation may manifest these characteristics. Advanced Persistent Threats (APT) due to their uniquely tailored capabilities, specific target set, and enduring nature exhibit high levels of both Mobility and Damage Potential. Consequently, coercive cyber operations that involve the use of APTs are treated as possessing these attributes. Identifying the CSO of an adversary, on the other hand, involves determining whether the SPC of the said actor is either high or low. High levels suggest a Positive CSO while low values are indicative of a Negative CSO. For these values, the paper employs Rivera's dataset that identifies states with high or low levels of SPC based on the Freedom House Index (Rivera, 2015). Finally, the affected layer of cyberspace is identified based on the characteristics of their respective CSOs. As mentioned previously, P-CSOs focus primarily on the availability and flow of information. Consequently, this suggests that the most important layer would be that of the Syntactic layer. In contrast, N-CSOs depend on the manipulation or theft of information. While these may also involve the Syntactic layer, it is ultimately the management of the Semantic layer that permits the achievement of such. With respect to the dependent variable, the outcome of coercion, the paper refers to the Objective Success field present in the Dyadic Cyber Incident Dataset (DCID) that indicates whether the objective of the initiator (e.g. Disruption, Espionage, or Coercion) was met (Valeriano & Maness, 2014).

Having considered the overall design and variable operationalization, the remainder of the section is dedicated to the case selection strategy. As the paper focuses on state-to-state interactions in cyberspace, the following constraints are placed on selecting the appropriate case. First, only instances of state-based or state-endorsed operations are considered. Second, only instances where operations are targeted against state-owned and state-operated assets are considered. Operations that affect government and military systems are thus in scope while those involving private industries are excluded. Third, only compellent coercive cyber operations are considered. This restriction to compellent activity is in place as compellence is generally thought of as being more difficult. If the arguments of the prevailing explanation are valid, then the use of highly mobile and damaging operations should make such threats more credible. Finally, cases are selected such that they are representative of the "cyber

revolution" thesis. Should the prevailing argument suffice, there ought to be little that the proposed alternative may add to the analysis of the case.

Selection & Analysis

With respect to the requirements for mobility and damage potential, the case of Stuxnet in 2010 serves to be highly illustrative and in favor of the "cyber revolution" thesis. Stuxnet – dubbed as the first "weaponized" malware – employed six (6) different vulnerabilities, had the ability to jump the air gap, and could inflict physical damage. Its employment to disrupt Iran's nuclear programme fits into the narrative of cyberspace as a threat to an adversary's strategic interests. However, Stuxnet had done little to disrupt Iran's nuclear ambitions. Later analysis revealed that while its unique feature-set endowed it with significant potential, the actual damage inflicted had not exceeded that of normal operational breakdown (De Falco, 2012; Iasiello, 2013; Lindsay, 2013).

While the post-incident analysis concluded that the overall physical damage caused by Stuxnet was minimal, it is unlikely that Iranian authorities would have concluded with absolute certainty that no other operation was presently threatening the remainder of its cyber infrastructure. Although details regarding the decision-making process at the time is unavailable, this argument is supported by subsequent actions of the regime. First, it is highly unlikely that Iranian authorities overestimated their own defensive capabilities as well as underestimated the capabilities of the suspected aggressors – later to be attributed to the United States and Israel. The fact that external expertise had been sought out to contain Stuxnet suggests limited capabilities on the part of the regime (De Falco, 2012). Furthermore, despite significant investment in the development of their own cyber capabilities (Ward, 2008), the need for external assistance hints at not only the complexity of this operation, but the vulnerability of their cyberspace at the time. Second, if the authorities had indeed felt the attack to be inconsequential, then what need would there have been for their aggressive pursuit of cyber capabilities post 2010? Moreover, why would there have been a need for a retaliatory operation if the damage itself was inconsequential?

The rationale above suggests that Iran, despite the outcome of Stuxnet, still viewed the operation as significant enough to cause a reassessment of its capabilities. However, not significant enough to alter its behavior with respect to its nuclear programme. If coercion aims to influence behavior by threatening costs, then it appears that the consequences of Stuxnet had not crossed a threshold. This casts doubt on the validity of the prevailing arguments calling for the use of highly mobile and damaging cyber operations. At the time, Stuxnet represented a revolutionary development in the capabilities of actors in this domain. One must inquire as to what activities that threaten cyberspace would have been significant enough to compel Iran to change its behavior. They key to answering this question rests on an understanding of how the Iranian regime perceives the domain. The nature of the Iranian regime makes it difficult to gain insight into the perceptions of key decision makers with

respect to cyberspace. Yet the few statements available, however, provide the necessary information to surface the regime's views with regards to cyberspace.

In March 2012, Ayatollah Ali Khamenei issued a call for the creation of a Supreme Council of Cyberspace noting that "*dramatic effects*" that the growing use of these technologies have had on the social dimension of human life (Khamenei, 2012). Moreover, General Behrouz Esbati of the Islamic Revolutionary Guard Corp notes in an interview in 2015 that cyberspace is composed of three layer: hardware, software, and "brainware". While the former two are self-explanatory, the later, he argues, refers to the "*establishment of goals in cyberspace, activity related to meaning and content, and types of analysis occurring in the cyber domain*" (Bucala & Pendelton, 2015). This definition allows the notion of "brainware" to be equated with that of the Semantic layer. Moreover, the general's views relative to his position suggests the importance of this component with respect to Iranian cyberspace.

The general later goes on to note that "*the creation and engineering of communications in the Internet can be turned into a threat; for example it is possible for you to Google something and for another individual to manage the meaning of the search results.*" This need to manage information cannot be attributed solely to the general as other elements of the Supreme Cyberspace Council are also required to exercise similar tasks (Bucala & Pendelton, 2015). Furthermore, this need to manipulate information suggests the presence of a Negative-CSO in effect within Iran. This is not entirely surprising given the level of Socio-Political Cohesion within Iran and the nature of the regime itself.

The arguments presented above, thusly, suggests the possibility that loss of control over information reflected by the Semantic layer challenges the objectives of the regime. With respect to the paper's arguments, this would suggest that in the case of Iran, coercion would most likely be more successful if aimed at hindering their ability to meet their N-CSO by launching operations aimed at the Semantic layer. This vulnerability is further suggested by events prior to Stuxnet. Specifically, this was reflected in the establishment of Internet censorship in response to political dissent in the early years of the 21st century and in the initiative to develop its own internal network that emerged after the 2009 Green/Twitter Revolution (Golkar, 2011; Rahimi, 2003). These examples support the argument that an understanding of the adversary's perception of cyberspace and its critical components may shed insight with respect to the nature of cyber operations required to achieve coercive success in the domain.

Building on the above argument, it is important to note predicating the success of coercion on an understanding of an adversary's vulnerability based on their objectives is not unique to this man-made domain. In his study of coercive air campaigns, Pape stresses the need to match coercive threats with an adversary's actions and objectives. Correct execution does not guarantee success if it does not introduce risk for the target. The example of Vietnam proves instructive in this case. Operations Rolling Thunder and Linebacker I and II were properly executed and maximized the full

technological potential of the US Airforce. However, the former failed to achieve its coercive goals as it was directed at assets of little value given the objectives of the adversary at the time. In contrast, the latter proved fruitful as it placed pressure on the adversary by threatening assets that it had deemed important at the time relative to its goals – conventional warfare directed at South Vietnam (Pape, 1996).

Conclusion

The adoption of cyber capabilities as one of the many instruments of national policy is well underway. More importantly, the increasing use of cyber operations as a coercive tool is manifesting itself in several long standing and emergent inter-state disputes. Unfortunately, the conceptualization of the dynamics of cyber coercion has yet to mature beyond speculations built on a sense of fear and dread that is encouraged by increasing societal dependencies on these technologies. While there may perhaps be some merit in the execution of coercive cyber operations that are fully able to exploit the intercedence between technology and strategic interests, the threat of systemic collapse, on its own, does not fully account for the success or failure of past cases. Interestingly, it appears that operations that are technologically simple and constrain the amount of damage they cause have proven to be the most fruitful.

This deviation from the expectations of the "cyber revolution" thesis calls for the need to further asses the strategic utility of coercive cyber operations. To this end, the paper has briefly presented an alternative account built on both the unique geography of cyberspace and varying perceptions of its importance. The paper has argued that careful consideration of these features is more likely to lead to coercive success rather than outright force that is manifested by highly mobile and damaging actions.

While the results presented herein are by no means definitive, it does raise the need to reassess events in cyberspace in a more theoretical light and emphasizes the necessity of evaluating the applicability of existing theories to study events in this domain. Despite its novelty, the study of cyberspace and its uses should not be built on hype over its characteristics, but rather; informed by empirical evidence framed through the lens of applicable theory.

Bibliography

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, *12*(2), 141–165.

Bucala, P., & Pendelton, C. (2015). Iranian Cyber Strategy: A View from the Iranian Military. Retrieved December 21, 2016, from http://www.irantracker.org/analysis/bucala-pendleton-iranian-cyber-strategy-esbati-interview-november-24-2015

De Falco, M. (2012). *Stuxnet Facts Report: A Technical and Strategi Analysis*. Tallinn. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf

Dunn-Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122. https://doi.org/10.1111/misr.12023

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, *30*(1), 28–38. https://doi.org/10.1109/MTS.2011.940293

Golkar, S. (2011). Liberation or suppression technologies? The internet, the green movement and the regime in Iran. *Australian Journal of Emerging Technologies and Society*, *9*(1), 50–70.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Hare, F. (2010). The Cyber Threat to National Security Why Cant We Agree. In *Conference on Cyber Conflict* (pp. 211–225). Tallinn: CCS COE Publications.

Healey, J. (2016). Winning and Losing in Cyberspace. In *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE.

Iasiello, E. (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. In *5th International Conference on Cyber Conflict* (pp. 451–468). Tallinn: NATO CCD COE.

Khamenei, A. (2012). The Formation and Appointment of Members of the Ruling Supreme Council of Cyberspace. Retrieved December 21, 2016, from http://farsi.khamenei.ir/message-content?id=19225

Libicki, M. (2010). *Cyberdeterrence and Cyberwar*. *Distribution*. https://doi.org/RAND

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

NATO CCDCOE. (2016). Cyber Definitions. Retrieved December 21, 2016, from https://ccdcoe.org/cyber-definitions.html

Pape, R. A. (1996). *Bombing to Win: Air Power and Coercion in War* (1st ed.). Cornell University Press.

Rahimi, B. (2003). Cyberdissent: The internet in revolutionary Iran. *Middle East Review of International Affairs*, *7*(3), 101–115.

Rivera, J. (2015). Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. *2015 7th International Conference on Cyber Conflict*, 7–24.

Saltzman, I. (2013). Cyber Posturing and the Offense-Defense Balance. *Contemporary Security Policy*, *34*(1), 40–63. https://doi.org/10.1080/13523260.2013.771031

Schaub, G. (2004). Deterrence, Compellence, and Prospect Theory. *Political Psychology*, *25*(3), 389–411. https://doi.org/10.1111/j.1467-9221.2004.00377.x

Schelling, T. (2008). *Arms and Influence*. Yale University Press.

Starr, S. (2009). Toward a Preliminary Theory of Cyberpower. In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and National Security* (pp. 43–88). Washington, D.C.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, *51*(3), 347–360. https://doi.org/10.1177/0022343313518940

Ward, C. (2008). Iranian Cyber Warfare Threat Assessment. Retrieved December 21, 2016, from http://www.defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/

Contact email: miguel.gomez@sipo.gess.ethz.ch