Global Security and Intelligence Studies

Volume 1
Number 2 *Spring 2016*

Article 5

2016

Arming Cyberspace: The Militarization of a Virtual Domain

Miguel Alberto N. Gomez
De La Salle University

Arming Cyberspace: The Militarization of a Virtual Domain

Miguel Alberto N. Gomez[A]

The increasing frequency of offensive cyberspace operations (OCOs) directed toward states, particularly the disclosure of Stuxnet in 2010 that appears to have been aimed at disrupting Iran's nuclear development program, has prompted a reassessment of state behavior in cyberspace. In the years since, states have gradually militarized cyberspace through the establishments of various programs that have framed this as a new domain of warfare. Yet despite the pace of these transformations, a unified theoretical understanding of this phenomenon continues to remain conspicuously absent. To date, scholars have attempted to explain such by highlighting the advantages offered by cyberspace while others have cited the growing fear-based rhetoric grounded by the increasing societal dependence on technology. Neither of these, however, can adequately explain why certain states have militarized while others have not despite predictions of such taking place. Consequently, this study, encompassing the period from 2011 to 2014, proposes that depolarizing these respective arguments may close the existing theoretical gap. In doing so, the study employs a quantitative analytical approach that examines how cyberspace had been militarized across states as a function of both strategic considerations and resource requirements which are both driven by rational choice and societal perceptions regarding this domain.

Keywords: *analysis, counterinsurgency, critical thinking, and operational environment*

Introduction

In the first decade of the twenty-first century, the discourse concerning cyber security in the global security landscape has shifted from criminal acts toward specific political and/or military events. Most notably, the discovery of the Stuxnet worm in June 2010 overturned previously held beliefs regarding offensive cyberspace operations (OCOs) (Farwell and Rohozinski 2011; Liff 2012a; Sanger 2012).

Stuxnet, believed to have been the first instance of a weaponized malware, was found to have caused disruptions in Iran's nuclear centrifuges at the *Natanz* facility (Farwell and Rohozinski 2011). Although the use of cyberspace in conjunction with on-going conflicts between states had not been novel at this point, this was the first instance wherein physical damage was deemed possible through actions in the virtual world. This signaled a reevaluation of the nature of events in cyberspace in terms of

[A] Assistant Professorial Lecturer, De La Salle University

doi: 10.18278/gsis.1.2.4

their professionalism, intent, and increasing complexity (Cavelty 2012; Valeriano and Maness 2013). In so doing, these changes support the *cui bono* logic of attributing these activities to states or state-sponsored organizations.

Consequently, the nature of these events assigns responsibility for responding to a state's civil defense and military apparatus (Cavelty 2012). Furthermore, the increasing number of suspected state or state-sponsored OCOs are believed to have accelerated the militarization of cyberspace with the adoption of military doctrines specific to this domain, the emergence of national cyber strategies, and the establishment of military units responsible for conducting warfare in cyberspace (Cavelty 2013; Luiijf and Besseling 2013; Ottis 2009; Nye 2014; Young 2009).Consequently, this study defines militarization as the adoption of cyberspace by the military in either an offensive or defensive manner (or both). As of 2013, however, of the 114 states with existing cyber programs, less than half (47) have involved their military—the remaining 67 have developed exclusively civilian programs (UNIDIR 2013).

If the threat of state or state-sponsored OCOs targeting critical infrastructure is indeed on the rise and if the actor task with responding to such is the military (Cavelty 2012), then what accounts for the varying levels of militarization across states? Simply stated, why do some states choose to militarize cyberspace to meet this perceived existential threat while others do not?

The existing literature provides two arguments that serve to explain this phenomenon. The first recognizes that the rising societal dependence on technology introduces an existential threat that may be exploited by states and thus requires cyberspace to be secured (Barnard-Wills and Ashenden 2012; Bendrath 2001; Hansen and Nissenbaum 2009; Starr 2009).[1] The second acknowledges the advantages that the cyber domain offers relative to land, air, and sea. Most notably, its asymmetric nature, plausible deniability, and its offensive advantage are factors for militarization (Libicki 2009; Liff 2012a; Saltzman 2013; Sharma 2010). While both offer probable reasons why states would choose to militarize cyberspace, certain realities remain unaccounted for.

Although technology has indeed become commonplace in the political, economic, and military spheres, we have yet to find a case wherein OCOs have been used in a catastrophic attack against critical infrastructure. At most, only partial and temporary disruptions were achieved (Lawson 2013; Rid 2012). For example, the case of Estonia in 2007 that resulted in the disruption of the financial and government services, while vast in scale was eventually contained without any long-term economic or financial damage.

With regards to the latter, although there are indeed advantages offered by this domain, both Iasiello and Valeriano point out that most instances of such have been viewed by their targets as mere nuisance and thus far have failed to coerce their targets as intended (Iasiello 2013; Maness and Valeriano 2015). Although Stuxnet in 2010 was claimed to have damage some of Iran's nuclear centrifuges, this had not hindered their

[1] The current cyber strategy released by the U.S. Department of Defense has dropped such alarmist language though (Farrell 2015).

enrichment program in the long run (Iasiello 2013). Furthermore, Chinese activities in cyberspace—although mostly in the form of cyber espionage—do not give credence to the argument that the attribution problem associated with cyberspace encourages its use (Passeri 2015). As argued by Valeriano and Maness, activities in cyberspace can be attributed to specific actors with a certain degree of confidence based on pre-existing rivalries and national interests (Valeriano and Maness 2015).

In light of the absence of a suitable explanation for state behavior in cyberspace, this study attempts to bridge the existing theoretical gap that does not account for the continued militarization of this domain despite the lack of success in using OCOs to shape state policies as a function of either technological capabilities or societal dependence. Specifically, the study posits that an understanding of the phenomenon depends not on a strict adherence to one of the aforementioned explanations. Rather, the study shows that the choice to militarize this domain is a function of both its technological advantages relative to other domains (e.g., land, sea, and air) and by the capabilities developed in response to perceived risk.

Consequently, the study is organized as follows. The succeeding section presents the reader with the theoretical framework adopted by this study. From this point, the study moves forward to discuss the specific methodology in use. This section also includes a brief discussion regarding the analytical approach applied to the study. The succeeding sections then present an analysis of the data collected as well as the result of the applied quantitative methods. The final section summarizes the results of the study and provides future direction for scholars wishing to expand on the results presented here within.

Theoretical Framework

To account for the variation of militarization across states requires a reassessment of the explanations offered by existing theories rather than seeing these as either invalid or mutually exclusive. In doing so, it must be acknowledged that the degree to which cyberspace is militarized is dependent on both strategic goals and the availability of resources rather than simply the ability or the need to use such resources for the sake of doing so (Gartzke 2013; Liff 2012a). This argument finds support in a number of studies. For instance, Valeriano and Maness have shown its frequent use among states that have pre-existing rivalries (Valeriano and Maness 2013). Their analysis suggests that states with existing regional rivalries use cyberspace as a means of signaling during periods of increased tension (Maness and Valeriano 2015).

In addition, both Andres and Axelrod further investigated the influence of rivalries vis-à-vis strategic objectives. Andres coins the term *inverted-militarized-diplomacy* in which policy makers utilize militarized assets (i.e., cyber weapons) to seize desired resources (e.g., proprietary information) while relying on diplomats to limit escalation (Andres 2014). Parallels can be drawn with the English use of privateers to challenge the position of Spain during the Elizabethan period. Since these individuals were not visibly agents of the English crown, the uncertainty resulting from this limited the possibility of escalation. Similarly, Axelrod and Iliev have developed a mathematical model predicting when states would engage in the use of cyber weapons. A crucial factor in such a decision is the expected gains relative to the resources invested in the development and use of such. Simply put, actors will only chose to utilize these assets if the expected gains is substantial enough to justify (1) the loss of the ability to re-use them (i.e., zero-day exploits) and/or (2) the possibility of escalation (Axelrod and Iliev 2014). This builds on the points raised by the previous authors arguing that strategic considerations provide the initial rationale for the militarization of this domain. As such, the following hypothesis is proposed:

H1: *States that experience a greater number of offensive cyberspace operations from rival states attain a higher level of militarization.*

While the literature supports the idea that strategic interests are crucial in militarizing cyberspace, one must also take into account the consequences of militarization. Liff argues that while states may have the technical capabilities and strategic interests to militarize cyberspace, the decision to do so is constrained by their conventional capabilities (Liff 2012a). This argument rests on two important points. First, cyberspace is a resilient domain. While states may engage in OCOs to weaken their rivals, whatever damage incurred is temporary—the nature of cyberspace limits, if not denies, the possibility of permanent damage to a target (Maness and Valeriano 2015). This perspective is grounded in the resilient nature of this domain coupled with declining costs associated with technologies that allows for the development of systems that, while still vulnerable, can be restored within a defined amount of time. Sharma points to this argument to account for the limited use of cyberspace as an instrument of warfare (Sharma 2010).

Second, the availability of a conventional option (e.g., an air strike) allows an aggressor to better signal his intent given the resilient nature of cyberspace (Lawson 2013; Liff 2012b; Stone 2013). This extends the previous point by arguing that gains achieved through actions in cyberspace are temporary and any further consolidation would require intimidation or coercion through other means. Stone argues that parallels may be drawn between the use of cyberspace and airpower during the Second World War wherein these act as complementary tools to other instruments of warfare (i.e., ground forces) (Stone 2013). Furthermore, Liff supports this argument by suggesting that conventional capabilities are needed to secure gains made in the cyber domain (Liff 2012a). As such, the following hypothesis is proposed:

H2: *States that attain greater hard power reach a higher level of militarization.*

While strategic considerations may contribute to the militarization of cyberspace, states intending to do so would require resources to support this undertaking. Furthermore, the mobilization of these resources has been achieved through fear-based rhetoric on the part of elites. Lawson posits that perceptions regarding societal dependence on technology contribute to the perceived existential threat originating from cyberspace (Lawson 2013). These threats are rooted at both the societal and technological levels given how this domain is viewed as both technological and societal constructs. As proposed by Barnard-Wills and Ashenden, cyberspace is built on networking information technologies that form the foundations of a domain that is shaped by the manner that *people and institutions, think, understand, and talk about this space* (Barnard-Wills and Ashenden 2012). Both the technological and social components are understood to have their own vulnerabilities that, in turn, introduce risk that need to be mitigated (Giles and Hagestad 2013; Hansen and Nissenbaum 2009). In her study, Cavelty identifies the use of the military and other civil defense organizations in responding to catastrophic attacks against critical infrastructure—the targets most often cited as those facing the greatest risk (Cavelty 2012). As such, the following hypotheses are proposed:

H3: *Increasing societal use of cyberspace increases militarization.*

H4: *Increasing technological risk associated with cyberspace increases militarization.*

Even if this two-tiered perception of cyberspace is accepted, the impact of the risk associated with cyberspace rests on its resonance across a wider audience. In her study, Cavelty identifies one of its referent objects as critical infrastructure (Cavelty 2012). Catastrophic attacks aimed at these would prompt their securitization. Furthermore, Hansen and Nissenbaum have identified three specific modalities under which such a securitization takes place: *hypersecuritization, everyday security practices, and technifications*. The first refers to large-scale disaster scenarios as a result of societal dependence on information and communication technology (ICT). While the second relates to how threats originating from cyberspace would impact an individual's day-to-day life (Hansen and Nissenbaum 2009). To be viewed as an existential threat, Sharma argues that the impact of activities in cyberspace must span these two modalities (Sharma 2010). While no single case has proven these scenarios as of yet, elites have employed these scenarios to call for the further militarization of cyberspace (Lawson 2011). As such, the following hypothesis is proposed:

H5: *Elite influence through speech acts increases militarization.*

It should be noted that this framework does not discount current explanations that are grounded on the advantages offered by this domain and by the existential fear surrounding it, but instead synthesizes these by insisting that the act of militarization does not occur independent of other factors. The militarization of this domain is mandated by a strategic need to do so and is enabled by the availability of resources as determined by the elite's ability to instrumentalize risk associated with the use of this domain.

Methodology

Case Selection

Given that no suitable dataset currently exists to capture the variation of cyberspace militarization across states, this study has constructed its own by utilizing a variety of open-source resources and is comprised of 88 unique observations. Given that militarization is viewed at the level of the state, the universe in question involves states with existing cyber programs. As of 2013, the United Nations Institute for Disarmament Research (UNIDIR) has identified a total of 114 states with existing cyber programs involving both the private and public sectors (UNIDIR 2013). In addition, the time period considered is from 2011 to 2014. The lower bound is set to 2011 as a result of changes in perception in response to the discovery of the Stuxnet worm in 2010. The data is lagged by 1 year to allow this to take effect. Furthermore, authors such as Cavelty observe that events such as Stuxnet have altered the perception of cyberspace from being a civilian domain to that of a military one (Cavelty 2013). Consequently, extending the study earlier than 2011 is not insightful given this change.

The cases sampled from this universe are instances of states that have an existing cyber program and have experienced OCOs attributed to either state or state-sponsored actors. The sampling strategy adopted is crucial for two reasons. First, by omitting cases attributed to cybercrime, the amount of noise from unrelated events is reduced. Second, threats originating from these state or state-sponsored actors result in the state being the referent object as oppose to cybercrime that affects individuals or private organizations, respectively (Cavelty 2013). Information regarding specific instances of OCOs are obtained from the *Hackmageddon* project—an open-source initiative that tracks cases of cybercrime and cyber warfare through multiple sources (e.g., news articles and industry reports) on a monthly basis (Passeri 2015). To identify valid instances of state or state-sponsored OCOs from this repository, the methodology proposed by Ottis is applied (Ottis 2009). All the identified cases that match the above-mentioned criteria are then aggregated to the level of the state.

It should be pointed out that two important (and inherent) limitations exist. First is reporting bias. The nature of these events limits the possibility of such reaching the public. Consequently, there is the possibility of underreporting the actual number of incidents that take place at the state level. The choice to rely on open sources allows for the broadest and most reasonable coverage. Second, the challenge of attributing the source and target of OCOs limits the accuracy of the data. Although Valeriano and Maness suggest that the existing interstate relationships could limit this problem, there continues to be no method to definitively identify actors short of aggressors and targets willingly disclosing information (Valeriano and Maness 2015).

Operationalization

In order to account for variations in cyberspace militarization, the dependent and independent variables represented in the previously defined hypotheses must be operationalized. Although the study employs pre-existing metrics to represent these variables, a number of these have been developed solely for this study due to the lack of existing metrics.

Cyberspace Militarization (Dependent Variable)

To date there are no existing studies that suggest a quantitative measure for the militarization of cyberspace. Consequently, this study employs artifacts that have been identified to be crucial for the military's involvement in cyberspace (Luiijf and Besseling 2013; Ottis 2009; Young 2009). These are as follows:

- A military doctrine or policy regarding cyberspace (*d*).
- A national cyber security strategy that recognizes state or state-sponsored cyber threats (*s*) and.
- A military and/or civilian unit(*s*) involved in to cyber defense and/or offense (*u*).

Each component is assigned a specific value and a weighted score is computed based on Equation 1. As the literature does not provide insight as to the precise weight to be given for each component, the study employs a near equal weighting scheme with an exception toward military doctrine or policy that is identified as playing a significant role (Young 2009). To this end, the components of this variable are scored based on the scheme indicated in Table 1.

It should be noted that the study is constrained by the availability of information in the public domain. Sources include the ETH Defense White Papers and National Security Strategies Series (ETH 2015), the NATO Cooperative Cyber Defense Center of Excellence (NATO CCDCOE 2015), the European Union Agency for Network and Information Security (ENISA 2015), the UNIDIR's Cyber Index report (UNIDIR 2013), and Luiijf and Besseling's study on national cyber security strategy (Luiijf and Besseling 2013).

Table 1. Militarization Scoring

Component	Score	Description
Military doctrine/policy	(1)	Has a dedicated doctrine/policy that recognize cyberspace as a unique domain of warfare or as a source of existential threats
	(0.5)	Has a separate doctrine/policy where cyberspace is recognized as a domain of warfare or as a source of existential threats
	(0)	Has no doctrine/policy that recognizes cyberspace as a domain of warfare or as a source of existential threats
National cyber security strategy	(1)	Has an existing national strategy recognizing state or state-sponsored OCOs as a threat
	(0.5)	Has an existing national strategy but does not recognize state or state-sponsored OCOs as a threat
	(0)	Has no existing national strategy
Cyber units	(1)	Has an existing military organization responsible for cyberspace
	(0.5)	Has an existing civilian organization responsible for cyberspace
	(0)	No existing organization responsible for cyberspace

$$\text{militarization} = d(0.4) + s(0.3) + u(0.3)$$

Equation 1. Cyberspace Militarization

Rivalry

To operationalize *H1*, the study employs dyadic rivalries between states that have experienced OCOs are identified using Klein's rivalry dataset (Klein 2006). While the dataset only covers periods up to 2001 (possibly limiting its reliability), the results from Valeriano and Maness' study that employed this dataset as well (encompassing periods from 2001 to 2011) appear to demonstrate its validity and reliability with respect to conflicts in cyberspace (Valeriano and Maness 2013). In measuring the significance of rivalry, the percentage of OCOs experienced from rivals relative to the total number of OCOs observed is used (see Equation 2). In cases where the sources of attacks could not be attributed, the study records this as having originated from a nonrival.

$$\text{rivalry} = \text{CNOs from Rivals} \div \text{Total CNOs}$$

Equation 2. Rivalry

Hard Power

To operationalize *H2*, the study employs national power as measured using the Composite Index of National Capability (CINC) present in the *Correlates of War version 4* dataset (Sarkees and Wayman 2010). While CINC is primarily a measure of hard power, it should not limit its validity since the existing literature refers specifically to conventional military capabilities when referring to state power vis-à-vis cyberspace (Liff 2012b). It should be noted, however, that the most recent CINC values are only until 2007.

ICT Use

To operationalize *H3*, societal dependence on ICT is captured through the *use sub-index* of the International Telecommunications Union's (ITU) *ICT development index*. The *use sub-index* measures the current usage of ICT within a given society and is a compounded score that integrates other measures such as *fixed broadband subscription, Internet access*, etc. (ITU 2013; 2014). The study employs the mean of this measure from 2011 to 2014.

Risk

As with militarization, there is currently no quantitative state-level measure for risk in cyberspace. To operationalize H4, the study applies the risk measurement formula (see Equation 3) usually employed by private organizations (SANS Cyber Defense 2012). For this study, the mean of malware infection rates from 2011 to 2014 per state is used as a proxy measure for threat, vulnerability, and impact. The presence of an infection is a manifestation of these three concepts (Microsoft Corporation 2015). These rates are based on infections identified in devices running Microsoft's operating system (Myslewski 2014). Given that the organization has >80% of the market share globally, this is an acceptable measure. The mean of Internet usage from 2011 to 2013 as measured by the ITU serves as the proxy for impact, the assumption being that the presence on the Internet increases the number of possible victims of infection (World Bank 2014). At the state level, the ITU's 2014 Global Cyber Security Index best represents countermeasures for these threats (ITU & ABI Research 2014). The result is then scaled from 0 to 1.

$$\text{risk} = (\text{threat x vulnerbaility x probability x impact}) \div \text{countermeasures}$$

Equation 3. Risk

The result of the above-mentioned formula represents what is referred to as residual risk or the amount of risk faced once the necessary steps to mitigate threats have been applied.

Elite Influence

Of the variables involved in this study, measuring the influence of elite speech acts is challenging to quantify. Moreover, there are no consolidated records concerning elite references to cyberspace. To operationalize *H5*, the ratio between references of elite and nonelite statements concerning policy change is used as a proxy. This measures the importance of the topic vis-à-vis the specific actor (GDELT Project 2013). These values are obtained through the *GDELT Project* that monitors broadcast, print, and web-based news sources and to date has over a quarter of a billion entries (Leetaru 2015). The primary limitations faced are the scope of information available to the *GDELT Project* as well as the accuracy of its automated systems that are used to classify the relevant actors in these documents.

Polity

The additional variable of polity from the *Polity IV* dataset that measures the level of democracy in a given state is applied as a control variable (Marshall, Gurr, and Jaggers 2010). Hare points out that regime type may impact how a state perceives threats from cyberspace (Hare 2010). Consequently, this may shift the referent object away from the state as noted by Cavelty (Cavelty 2013). The study employs the mean of the *polity 2* indicator from 2011to 2014.

Analytic Approach

To confirm the possible causal relationship between the dependent (*Militarization*) and independent (*hard power, risk, ICT use*, etc.) variables that account for the variation of cyberspace militarization, the study adopts a two-step quantitative approach.

To trace causal paths between the variables, the study implements a Bayesian Causal Network (BCN) to provide a graphical representation of the causal links between variables. The use of BCNs allow for (1) a graphical output that is easy to interpret, (2) a measure that shows a positive, negative, or absent causal relationship, and (3) mitigates the impact of small sample bias (Kalisch and Mächler 2011). BCNs, however, do not offer a measure of the statistical significance. Furthermore, certain BCN techniques require that there be no hidden variables and that all variables involved in the causal relationship have been accounted for. Although this may appear to be constrictive, this prerequisite demands that the theoretical framework be as rigorous as possible and serves to ensure robust results.

Once the causal structure has been established through the previous method, the study then applies cluster analysis. The reason for this is twofold. First, if the previously established causal links are valid, then what should result are unique clusters in which the respective values of both dependent and independent variables are unique for each cluster—thus confirming the previous findings. For the purpose of this study, the expectation maximization (EM) clustering algorithm is employed as it accounts for the possibility unobserved variables (Bilmes 1998). This is meant to address the constraints imposed by the first stage in the analysis. Second, aggregating individual states into unique clusters allows for the analysis of how dependent variables vary across these groups. Since clustering maximizes the difference between clusters while minimizing differences among its members, this results in each cluster representing a unique case with each cluster member (i.e., state) serving as individual observations. This allows for the possibility of applying qualitative techniques such as the method of similarity/difference to confirm the causal relationships. The difference between variables across clusters is measured through a simple two-group *t* test on their respective means.

Once the validity of these clusters is established, it confirms the causal relationship derived by the first step. The result would then either support or refute the proposed hypotheses that explain the process of the militarization of cyberspace.

Results and Analysis

Summary Statistics

The resulting dataset produced for this study identifies 88 unique states with existing cyber programs that had also experienced OCOs within the defined period. Table 2 presents the summary statistics of the dataset and from this, several key observations are made. Beginning with the level of militarization across states it can be stated that while most states have engaged in one form of this or another, there is as of yet no global trend toward the militarization of cyberspace. With a mean of 0.447 and by analyzing the specific components of the scores relevant to this variable, it can be said that most states have focused on establishing military and/or civilian units that are responsible for cyberspace in response to their respective cyber security strategies.

Table 2. Cyberspace Militarization Summary Statistics

	Mean	Median	Maximum	Minimum
Risk	0.119	0.073	1.000	0.000
ICT use	3.757	3.632	8.233	0.217
Hard power	0.011	0.003	0.200	0.000
Elite influence	0.609	0.624	1.000	0.078
Rivalry	0.148	0.000	1.000	0.000
Polity	4.966	8.000	10.00	-10.00
Militarization	0.447	0.450	1.000	0.000

There are, however, fewer states (41%) whose existing military doctrine recognize cyberspace as a unique domain of war. This suggests that despite the growing number of OCOs attributed to state or state-sponsored actors, less than half believe this to be a new domain of warfare. A similar pattern is seen with regards to their respective national cyber strategies wherein only 31% acknowledge state and state-sponsored OCOs.

Moving the discussion forward, several key observations can also be established regarding the independent variables. Concerning the risk faced by states, the sample shows this to be skewed to the right. Its distribution, along with a mean value of 0.12 and a median on 0.07 suggests that, despite the perception of increasing risk, most states have been able to mitigate threats from cyberspace. Moreover, the fact that *ICT use* and *elite influence* appears to be normally distributed (see Figure 1) in the sample suggests the absence of bias in favor of states that are better able to address threats from cyberspace as an explanation for how *risk* has been represented or elites that have ardently vocalized the need to secure this domain. In addition, the mean value of 3.76 and maximum value of 8.23 for *ICT use* also suggests that despite the increasing societal dependence on these technologies it cannot, as of yet, be said to be pervasive at a global level. Consequently, it may be argued that the perceived threat originating from the technological component of cyberspace has yet to reach a critical point, thus accounting for the level of militarization captured by this dataset.

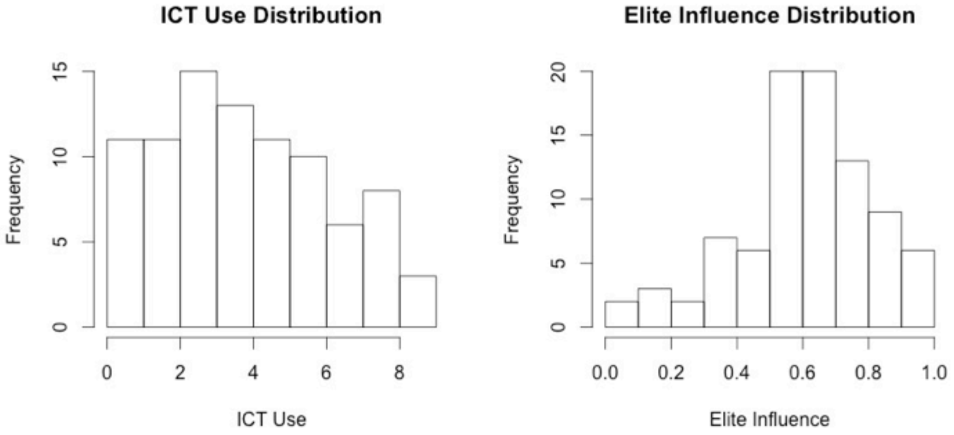

Figure 1. ICT Use and Elite Influence Distribution

Interestingly, the variable *Polity* appears to be skewed to the left while that of *Hard Power* is skewed to the right (see Figure 2). Although authoritarian regimes are represented in the data, the majority of the observations are of democratic regimes. In addition, most of the observations suggest middling to weak military capabilities (i.e., Hard Power). These two points are crucial, particularly in the context of Hare's study wherein such states are vulnerable to highly disruptive OCOs that target their critical infrastructure (Hare 2010). If this is the case, Cavelty's model predicts further militarization of cyberspace (Cavelty 2013). Following this line of reasoning, if militarization is a function of both *Polity* and *Hard Power* alone, then one should expect a higher mean value for this variable.

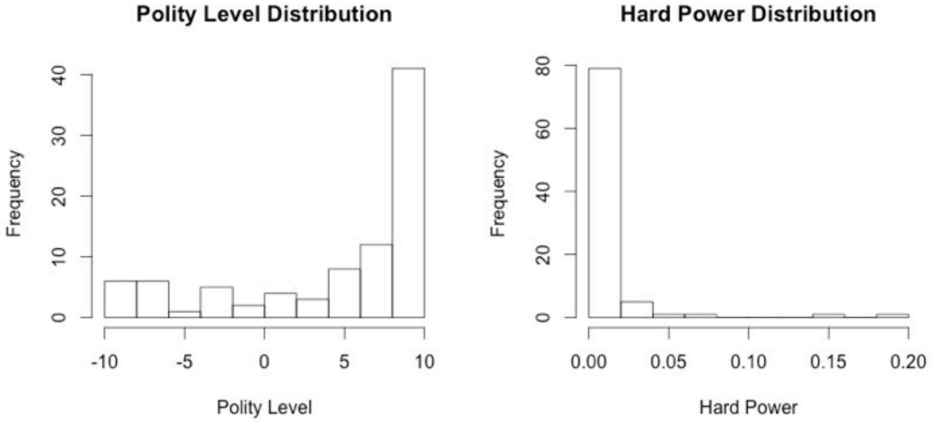

Figure 2.Polity and Hard Power Distribution

Finally, it should be noted that fewer instances of OCOs originating from rivals have been observed in contrast with Valeriano and Maness' study. This deviation could be explained by the manner in which the population was sampled compared to the previous study. For Valeriano and Maness' dataset, only cases of state initiated actions were included in the dataset. Instances of state-sponsored activities were kept at a minimum (Maness and Valeriano 2015). In doing so, the sampling may have been indirectly limited to states with prominent rivalries, thus accounting for the characteristic of this variable in their study.

Causal Relationship

Before proceeding with reviewing the causal relationship between the dependent and independent variables, additional information may be gleaned by inspecting how these are associated with one another. Table 3 shows the respective correlation coefficients (Pearson's Correlation) along with their *p* values.

Table 3. Correlation Table

Independent Variables	Dependent Variable	Correlation Coefficient	*p* Value
Risk	Militarization	–0.433	2.575e–5
Rivalry	Militarization	0.070	5.183e–1
Hard Power	Militarization	0.435	2.280e–5
Elite Influence	Militarization	–0.026	8.113e–1
ICT Use	Militarization	0.472	3.356e–6
Polity	Militarization	0.285	7.128e–3

With the confidence interval set to 0.95, it can be seen that only *risk*, *hard power*, *ICT* use and *polity* are statistically significant in terms of their relationship with *militarization*. The latter three can be said to be positively associated with *militarization* while the former (*risk*) is negatively associated. If applied to the current hypotheses, the association displayed by *hard power* and *ICT use* appears to conform to the expectations of *H2* and *H3* that suggest the expected behavior of these two variables. On the other hand, *risk* appears to contradict H4 that expects a positive association between *militarization* and *risk*. This, however, could be explained by the manner in which this variable was operationalized. Since the metric is obtained by using existing countermeasures as the divisor, lower risk suggests greater capabilities in cyberspace. These capabilities may be re-tasked or re-developed to support the militarization of this domain, thus explaining the negative relationship. Finally, the coefficients and *p* values of the remaining variables suggest a lack of association between these and the dependent variable, possibly discrediting hypotheses *H1* and *H5*. However, since correlation does not imply causation, further tests are required to evaluate the hypotheses.

Table 4. Causal Relationship vis-à-vis *Militarization*

Variables	**Linked to** *Militarization*	**Causal Strength**
Risk	Yes	–0.765
ICT use	Yes	0.053
Hard power	Yes	4.080
Elite influence	No	–0.032
Rivalry	No	0.058
Polity	No	0.011

The outcome of generating a BCN is seen in Table 4. The first column on the left-hand side identifies the independent variables. The second indicates whether or not there is a direct causal link between the independent variables and the dependent variable (*militarization*). The right-most column lists the respective strength of the causal link between the dependent and independent variables. In this case a value of zero (or near zero) would indicate an absence of a causal relationship. A positive or negative value for this column indicates the direction of the causal relationship. From Table 4, several relevant observations can be established. First, the absence of a link between the variables measuring *rivalry*, *elite influence*, and *polity* and that of *militarization* suggest that these variables do not contribute to the emergence of this phenomenon. Referencing the association of *rivalry* and *elite influence* to that of *militarization* in Table 3, the previous step (correlation) had already shown an absence of a relationship. Furthermore, the causal strength between these two variables to that of the dependent variable (see Table 3) are near zero, thus indicating an absence of such a relationship and any immediate causal influence. This, however, does not indicate that these variables do not play an indirect role in the militarization of this domain. Expanding the dataset by including more observations may change the result given the probabilistic nature of BCNs.

Second, both variables measuring *risk* and *hard power* appear to have a direct causal relationship with that of *militarization*. The previous analysis of the association between these two variables to that of the dependent variable coincide with the direction and causal strength indicated in Table 4. It illustrates the negative relationship between *risk* and *militarization* and the positive relationship with that of *hard power*. Curiously, *ICT use* that had a significant association with *militarization* has a near zero value in Table 4. This suggests that while there appears to be a causal link between *ICT use* and *militarization*, it is not as significant as the other two variables. Simply stated, *ICT use* is not prominent enough to significantly influence the militarization of cyberspace but still contributes to the militarization of cyberspace in some way. But as with the previous point, the influence that *ICT use* may play may change assuming that these tests are redone with a greater number of observations.

Result Verification

At this point, the inferred causal relationship appears to confirm *H2*, *H3*, and *H4* (represented by *hard power*, *risk*, and *ICT use*, respectively) while rejecting the remaining hypotheses. In effect, the initial results support the proposition that both strategic considerations and risk perception directly influence the variation of cyberspace militarization. However, confirming the causal links can only be achieved if the relevant variables on a state level are clustered such that unique values of *militarization* would emerge in the resulting groups. The result of which can be seen in Table 5.

Table 5. Cluster Summary

Group Number	Group Size	Risk	ICT Use	Hard Power	Militarization
1	7	0.023	5.047	0.077	0.864
2	67	0.091	3.499	0.005	0.429
3	14	0.299	4.345	0.001	0.325

In keeping with the inferred causal chain, three groups with unique levels of *militarization* are present.[2] These three groups may be classified as having high (0.67–1), medium (0.34–0.66), and low (0–0.33) militarization of cyberspace. It should be pointed out that in the process of evaluating the uniqueness of each group with one another, *ICT use* had been shown to not be statistically unique across the groups. This finding reinforces the weak causal strength that was previously established for this variable and allows for the rejection of *H3*.

In contrast, the measures for *risk* and *hard power* vary across these three groups and serves to explain the respective levels of *militarization*. Beginning with Group 1 that is represented by the United States, this has the highest level of *militarization* among the three groups. Most notably, this group's variables measuring *risk* and *hard power* are the lowest and highest among the three, respectively. The level of risk associated with members of this group suggests significant capabilities in mitigating cyber-borne threats. If compared to that of the other groups, the militarization of cyberspace decreases as risk increases—confirming earlier findings. While this does not immediately prove *H4*, as this hypothesis requires risk to be high for militarization to follow in the same direction, it may be argued that as risk increases, the steps taken to reduce such would require an investment in technologies and processes that could, in turn, be used to increase the militarization of cyberspace. As such, *H4* cannot be rejected.

In addition, it is also observed that as the value of *hard power* is reduced so does that of *militarization*. Again, this confirms the previous findings and is aligned with hypothesis *H2*, thus this hypothesis is retained.

[2] The variables for each group have been subjected to *t* tests to evaluate whether they are statistically different from one another.

The interaction between *risk* and *hard power* is made more apparent if compared across the three groups. Starting with the case of Group 1 and Group 2, there is a stark difference between *risk* (by a factor of 4) and *hard power* (by a factor of 15). While it could be said they are experiencing comparable levels of risk, the conventional military capabilities of Group 1 is significantly higher than that of Group 2 and could account for the higher value for *militarization*. In contrast, Group 2 and Group 3 have nearly identical levels of *hard power* but the risk faced by Group 2 is less than the latter by a factor of 3 and could account for the latter's lower levels of *militarization*.

Table 6. Inter-Group Similarities

Group Number	Risk	ICT	Power	Militarization
1		X		
2		X		X
3		X		X

Apart from the rationale derived from the causal chain that had been previously established. The resulting values for the level of cyberspace militarization could also be accounted for by Liff's model seen in Table 7. It should be pointed out that this model only takes into account the conventional military capabilities of the said actors and does not explicitly account for the risk faced in cyberspace. To integrate risk in the process of militarization, the model developed by Hare is relevant but requires one to reconsider the possible influence of polity—acknowledging the correlation identified earlier in this section. This model is illustrated in Table 8.

Table 7. State Interactions (Liff 2012a)

State Interaction	**Characteristics**
Strong state versus superpower	• OCOs provide only marginal advantages and useful only for difficult to attribute attacks against civilian or military infrastructure • A superpower may perceive vulnerability in cyberspace and may not initiate aggression • OCOs act as a counter-force or counter-value weapon against conventional capabilities
Weak state versus strong state/ superpower	• Weak state lacks the ability to follow through from the OCO with conventional attacks • Weaker state could launch OCOs against stronger adversary but is limited due to fear of possible escalation through conventional means • OCOs from strong state/superpower may not occur due to lack of targets in cyberspace
Weak state versus weak state	• Lack of conventional capabilities would shift conflict over to cyberspace • Limited conventional capabilities would limit escalation

Table 8. Cyber Vulnerabilities and Types of States (Hare 2010)

		Socio-Political Cohesion (C)	
		Weak (W)	**Strong (S)**
Power (P)	**Weak (W)**	De-stabilizing political actions in cyberspace, attacks on Internet Infrastructure, criminal activities	DDoS and other major attacks on critical-infrastructure
	Strong (S)	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

With these models on hand, the proposed relationship between risk and hard power are further strengthened. Starting with Group 1 and Group 2, the first mode of interaction could be use to explain the current level of militarization (see Table 7). As both groups face relatively comparable levels of risks (see Table 6), the greater conventional capabilities of Group 1 states would prompt these to view cyberspace as an alternative platform from which to initiate aggression and would thus invest in this domain. In contrast, Group 2 with lower conventional capabilities would militarize cyberspace as a means to counter possible aggression from Group 1 states. In terms of the risk these two groups face, Group 1 is classified under the P-S/C-S quadrant while Group 2 would be considered in the P-W/C-S quadrant based on Table 8. In both these cases, the solutions required to mitigate these are similar to one another and could thusly explain the similar values for risk between these two groups.

In contrast, the relationship between Group 2 and Group 3 follows the second interaction more closely. The greater conventional capabilities of Group 2 could influence it to develop additional capabilities in cyberspace. Group 3, on the other hand, would invest limited capabilities in cyberspace due to either (1) technological limitations or (2) fears of possible retaliation from stronger states. Lower levels of *militarization* for Group 3 could also be attributed to the risk it faces. Using Hare's model in Table 8, Group 3 states would be found in the P-W/C-W quadrant wherein similar threats from the other quadrants are present, but with the addition of de-stabilizing political actions. What this suggests is that rather than investing in external capabilities aimed toward other states, Group 3 states could focus instead on internal security and censorship (Giles and Hagestad 2013; Hare 2010).

Collectively, the quantitative analysis provided in conjunction with Hare and Liff's models explain how both *risk* and *hard power* could influence the level of *militarization*. But where then does this leave the growing use of ICT? Although it cannot be denied that there continues to be a gap between the prevalence of ICT between certain states (ITU 2014), this disparity does not appear to account for the choice to militarize cyberspace. This is to say, greater societal dependence on such technologies does not result in the militarization of this domain. The fact that relatively few states have included cyberspace in their respective military doctrines supports this claim. A better explanation as to why *ICT use* does not appear to significantly influence *militarization* is the uniform nature of the underlying technologies.

While the degree of use may differ from one society to another or between states, the manner in which such technologies function remain to be the same. A computer in the United States does not operate differently from one in Russia. The difference lies in the ability of certain actors to better understand how these technologies function in order to maximize their use. Phrased differently, the intellectual capability of a society may matter more than the prevalence of ICT. This argument finds support in the fact that, as the data shows, states that face lower risk (through better countermeasures) have a higher level of *militarization*. Furthermore, one has also to take into account the degree with which ICT has been integrated into society. As shown in Table 2, most states have adopted a moderate level of *ICT use*. This suggests that the level of dependence on these technologies have yet to reach a point wherein cyberspace may be used as a means to inflict wide-ranging damage as perceived by Sharma (2010). Consequently, these two reasons could account for the level of similarity and the low degree of influence this variable has on the process of militarization.

Conclusions and Future Direction

The growing number of OCOs being attributed to state or state-sponsored actors demands a better understanding of the underlying factors that result in the militarization of cyberspace. While the existing literature posits two seemingly incompatible arguments centered on either fear-based rhetoric or rational choice, the study has demonstrated that both these factors account for the varying levels to which cyberspace has been militarized across states.

On the one hand, while increasing societal use of information communication technologies have led to greater risks associated with these technologies, the capabilities developed that are necessary to mitigate such could similarly lead to the transform the domain of cyberspace for use in warfare. Aside from the re-tasking of defense technologies, there is now the appearance of technologies once associated with the criminal elements of cyberspace in OCOs attributed to state or state-sponsored actors. The malleability of this technology supports the argument that increasing use alone does not account for the militarization of this domain, but rather the ability to maximize the functionality provides those with this skillset to expand beyond the traditional domains of air, land, and sea.

Equally important—and thus linking the two existent theories—is the continued relevance of conventional military capabilities vis-à-vis the use of cyberspace. While there is no doubt as to the advantages offered by this virtual domain, namely its asymmetric characteristics, low cost of entry, and challenges of attribution; these exist in conjunction with the stated policy goals of a state. The ability to employ this domain is dependent on conventional military capabilities to consolidate whatever gains were obtained in the process. Although it would be theoretically possible to utilize OCOs to disrupt a state's critical infrastructure in times of war, the impermanence of the damage caused requires additional resources to be brought to bear in order to force a change in policy or behavior of a given adversary.

Viewed as the causal explanations for the militarization of cyberspace, the risk faced by a state may be understood as the catalyst that encourages the militarization of this domain. However, without conventional military capabilities that could be used to apply constant pressure on one's adversaries, viewing OCOs as a *revolution in military affairs* is of limited value.

With this in mind, what role do the other aspects (e.g., regime type, rivalry, and elite influence) identified by the literature have on militarization? Although the study has not demonstrated that these to have a direct causal influence on militarization, this does not suggest that no relationship exists. As previously mentioned, the nature of the quantitative techniques applied could lead to differing results if the number of observations is increased. Regime type, for instance, could influence the type of risk faced by states and, in turn, influence the technologies developed to meet these risk. Hare's model captures this and is seen clearly in cases of states such as that of the United States and the People's Republic of China (PRC). The former perceives threats to its critical infrastructure and other services in cyberspace. Consequently, this prompts the development of technologies to ensure resilience and pro-active prevention of disruptive events. The latter, in contrast, is concerned with dissent and political activism in cyberspace. Consequently, this results in the emergence of censorship technologies that do not translate directly to offensive capabilities in cyberspace—though espionage-related capabilities would benefit from these (Giles and Hagestad 2013; Hare 2010).

Similarly, perceived risk originating from internal threats could account for the decision to engage (or not) in OCOs against other rival states. However, cases such as that of the PRC do not follow this line of reasoning as the most prominent of their activities in this domain have been directed against their military, political, and economic rivals.

Lastly, the influence of elites in the militarization of this domain could, in the view of authors such as Nissenbaum, be constrained by a lack of understanding of its nature and the continued lack of synergy between experts in technology and national policy (Hansen and Nissenbaum 2009). This would lead to a situation wherein political elites could, and do, vocalize the dangers posed by cyberspace but lack the proper understanding of how to apply these technologies as a tool to support national policies and goals.

The manner in which states conceptualize cyberspace at this point in time finds parallels with that of the mid-twentieth century and the advent of nuclear war. While the technology of the time offered to revolutionize warfare, few understood the implications of such and the extent with which these would alter the relationship between states and their respective military strategies.

References

Andres, Richard B. 2014. "Inverted-Militarized-Diplomacy: How States Bargain with Cyber Weapons." *Georgetown Journal of International Affairs* 4: 119–129.

Axelrod, Robert, and Rumen Iliev. 2014. "Timing of Cyber Conflict." *Proceedings of the National Academy of Sciences* 111 (4): 1298–1303. doi:10.1073/pnas.1322638111.

Barnard-Wills, D., and D. Ashenden. 2012. "Securing Virtual Space: Cyber War, Cyber Terror, and Risk." *Space and Culture* 15 (2): 110–123. doi:10.1177/1206331211430016.

Bendrath, Ralf. 2001. "The Cyberwar Debate Perception and Politics in U.S. Critical Infrastructure Protection The Information Society as Risk Society." *Information & Security* 7: 80–103.

Bilmes, Jeff a. 1998. "A Gentle Tutorial of the EM Algorithm and Its Application to Parameter Estimation for Gaussian Mixture and Hidden Markov Models." *International Computer Science Institute* 4 (510): 126. doi:10.1.1.119.4856.

Cavelty, Myriam D. 2012. "The Militarisation of Cyberspace?: Why Less May Be Better." In 4th International Conference on Cyber Conflict, eds C. Czosseck, R. Ottis, and K. Ziolkoswki. Tallinn, Estonia: NATO CCD COE, 141–153.

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

ENISA. 2015. "National Cyber Security Strategies in the World." https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

ETH. 2015. "Defense White Papers and National Security Strategies." http://www.isn.ethz.ch/Digital-Library/Publications/Series/Detail/?id=154839.

Farrell, Henry. 2015. "What's New in the U.S. Cyber Strategy?" *The Washington Post*. http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/.

Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53 (October): 23–40. doi:10.1080/00396338.2011.555586.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73. doi:10.1162/ISEC_a_00136.

GDELT Project. 2013. "GDELT—Data Format Codebook v1.03." GDELT Project.

Giles, Keir, and William Hagestad. 2013. "Divided by a Common Language?: Cyber Definitions in Chinese, Russian and English." In *5th International Conference on Cyber Conflict*. Tallinn, Estonia: NATO CCD COE, 413–429.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155–1175.

Hare, Forrest. 2010. "The Cyber Threat to National Security Why Cant We Agree." In *Conference on Cyber Conflict* ed C. Czosseck and K. Podins. Tallinn, Estonia: CCS COE Publications, 211–225.

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

ITU. 2013. "Measuring the Information Society Report." Geneva, Switzerland: ITU.

ITU. 2014. "Measuring the Information Society Report." Geneva, Switzerland: ITU.

Kalisch, Markus, and M. Mächler. 2011. "Causal Inference Using Graphical Models with the R Package Pcalg." *Journal of Statistical Software* 47 (11): 1–26.

Klein, J.P. 2006. "The New Rivalry Dataset: Procedures and Patterns." *Journal of Peace Research* 43 (3): 331–348. doi:10.1177/0022343306063935.

Lawson, Sean. 2011. "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History." *Mercatus Center George Mason University Working Paper* 11-01 (2011).

Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10 (1): 86–103. doi:10.1080/19331681.2012.759059.

Leetaru, Kalev H. 2015. "GDELT Project."

Libicki, Martin C. 2009. "Sub Rosa Cyber War." *In The Virtual Battlefield: Warfare*, eds Christian Czosseck, and Kenneth Geers. Amsterdam: IOS Press, 55–65.

Liff, Adam P. 2012a. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (March 2015): 401–428. doi:10.1080/01402390.2012.663252.

Liff, Adam P. 2012b. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401–428. doi:10.1080/01402390.2012.663252.

Luiijf, Eric, and Kim Besseling. 2013. "Nineteen National Cyber Security Strategies." *International Journal of Critical Infrastructures* 9 (1): 3–31.

Maness, R.C., and B. Valeriano. 2016. "The Impact of Cyber Conflict on International Interactions." *Armed Forces & Society* 42 (2): 301-323. doi:10.1177/0095327X15572997.

Marshall, Monty G., Ted Robert Gurr, and Keith Jaggers. 2010. "Polity IV Project: Political Regimes and Transitions, 1800–2009." *Polity*.

Microsoft Corporation. 2015. "Microsoft Inteligence Report." http://www.microsoft.com/security/sir/default.aspx.

Myslweski. R, 2014. "Windows Hits The skids, Mac OS X On The Rise." *The Register*. http://www.theregister.co.uk/2014/03/15/windows_desktop_and_laptop_market_share_dips_below_90_per_cent/.

NATO CCDCOE. 2015. "Cyber Security Strategy Documents." https://ccdcoe.org/strategies-policies.html.

Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities."

Ottis, Rain. 2009. "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability." In *8th European Conference on Information Warfare and Security*, ed H. Santos. Lisbon, Portugal: ACI, 177–182.

Passeri, Paolo. 2015. "Hackmageddon." http://www.hackmageddon.com/.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (3): 5–32.

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

Sanger, David E. 2012. “Obama Order Sped Up Wave of Cyberattacks Against Iran.” The New York Times.

SANS Cyber Defense. 2012. “Insider Threat Risk Formula: Survivability, Risk, and Threat.” Boston, MA: SANS Institute.

Sarkees, Meredith Reid, and Frank Wayman. 2010. *Resort to War: 1816–2007*. Washington, DC: CQ Press.

Sharma, Amit. 2010. “Cyber Wars: A Paradigm Shift from Means to Ends.” *Strategic Analysis* 34 (1): 62–73. doi:10.1080/09700160903354450.

Starr, Stuart. 2009. “Toward a Preliminary Theory of Cyberpower.” In *Cyberpower and National Security,* eds Franklin Kramer, Stuart Starr, and Larry Wentz. Washington, DC: Potomac Books, 43–88.

Stone, John. 2013. “Cyber War Will Take Place!” *Journal of Strategic Studies* 36 (1): 101–108. doi:10.1080/01402390.2012.730485.

UNIDIR. 2013. *The Cyber Index—International Security Trends and Realities*. New York: UNIDIR.

Valeriano, Brandon, and Ryan Maness. 2014. “The Dynamics of Cyber Conflict Between Antagonists, 2001–2011.” *Journal of Peace Research* 51 (3): 347-360.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities. Cyber War Versus Cyber Realities*.

Young, Mark D. 2009. “National Cyber Doctrine?: The Missing Link in the Application of American Cyber Power.” *Journal of National Security Law & Policy* 7: 173–196.