Realism and Cyber Conflict: Security in the Digital Age

https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

ANTHONY CRAIG AND BRANDON VALERIANO, FEB 3 2018

This is an excerpt from *Realism in Practice: An Appraisal*. An E-IR Edited Collection. Available worldwide in paperback on Amazon (UK, USA, Ca, Ger, Fra), in all good book stores, and via a free PDF download.

Find out more about E-IR's range of open access books here.

With the proliferation of Information and Communication Technologies (ICTs), cyber security has become both a major source of concern for policy-makers and of great interest to scholars of international relations. From the financial loss to businesses through cyber crime, the theft of classified government data, or the targeting of critical infrastructure, cyber security poses a significant challenge to the economic and national security of countries globally. Cyberspace is now considered the fifth domain of warfare after land, sea, air, and space (Economist 2010), and traditional frameworks can help us understand this relatively new form of conflict.

Realism has long been a dominant paradigm in the international relations field and is based on a general set of assumptions about international politics: that states are the most important actors, who operate as independent units within an international system lacking centralised authority, and rationally pursue their self-interest to assure power and security (Schmidt 2002, 9). The emerging cyber security field exhibits a resurgence of realist-influenced perspectives with a focus on security and competition, the distribution of power, the advantage of offence over defence, and the benefits of deterrence strategies, thus offering an opportunity to evaluate realism's role in these debates.

In this chapter, we appraise the utility of realism in explaining international cyber politics. We provide an overview of realist theory and how it relates to cyber security before addressing a set of specific realist-influenced topics within the current cyber security discourse. By evaluating the evidence surrounding each, we assess the relevance of realism as a descriptive and prescriptive theory of state behaviour in the cyber domain. We argue that, although realism can help in raising key issues in cyber security, overall the perspective lacks the ability to explain the dynamics of cyber conflict.

Realism and Cyber Security

The realist tradition can be traced back to Thucydides' analysis of the Peloponnesian war in the 5th century B.C. where he emphasised the amoral nature of international politics and the importance of power to political survival (Vasquez 1995, 9-19). However, its articulation into a distinct theory of international relations can be attributed largely to Hans Morgenthau (1948) who focused on the struggle for power between rationally-acting, self-interested states.

Within neorealism, established in the 1970's, there is a divide between defensive and offensive realism. Both agree that survival is the state's primary motive, but for defensive realists, most states are status quo powers that aim towards a balance of power thereby maintaining a stable international system (Waltz 1979). Offensive realists, on the other hand, argue that states aim to maximise their power to ensure their survival in an anarchical system (Mearsheimer 2001). The most recent strand of realism, neoclassical realism, explains state behaviour not purely on structural factors, but also domestic level variables including the perceptions and misperceptions of decision makers (Ripsman et al. 2016).

Realism has been challenged for its inability to explain state behaviour or offer productive policy guidance. For example, several studies point to the lack of evidence that states act in accordance with balance of power logic, a prominent hypothesis within the realist literature (Rosecrance and Stein 1993, 10, 17-21; Schroeder 1994). Its contradictory predictions and lack of empirical progress leads Vasquez (1997) to condemn realism as a 'degenerative' rather than 'progressive' paradigm. Furthermore, statistical studies suggest the factors that realists argue increase national security, such as military build-ups and alliances, are often counterproductive and increase the likelihood of conflict (Senese and Vasquez 2008). Nevertheless, with its focus on security and conflict issues, realism appears to be the natural go-to theory for elucidating pressing cyber security issues.

The study of cyber conflict is generally thought to have begun when Arquilla and Ronfeldt (1993) developed the concepts of 'cyberwar' and 'netwar' and predicted a transformation of warfare in line with rapid advances in ICT. This form of conflict takes place within cyberspace, an environment defined simply as 'all of the computer networks in the world and everything they connect and control' (Clarke and Knake 2010, 70). Cyber conflict refers to 'the use of computational technologies in cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities' (Valeriano and Maness 2015, 32). It is these politically motivated types of interactions that we focus on because they directly impact national security.

Cyber threats are today perceived as a top national security concern as governments warn against attacks against vulnerable critical infrastructure. In 2012, for instance, the then US Defence Secretary warned of a cyber 'Pearl Harbor' against the power grid or the financial system, both of which are reliant on computer networks for their operation (Bumiller and Shanker 2012). According to a 2016 survey, 73 percent of Americans believed cyber terrorism presented a 'critical threat' to the United States (McCarthy 2016). Some commentators such as Clarke and Knake (2012) agree that cyberwar is a very real and pressing threat to national security, yet several scholars argue, to the contrary, that the threat is exaggerated. Rid (2013) writes that cyber war does not represent true violence in the Clausewitzian sense and is unlikely to in the future, while Valeriano and Maness (2015) demonstrate empirically the rare incidence and low severity of cyber conflict between rival states. Others have used securitisation theory to explain the heightened threat perception we currently witness (Cavelty 2008; Hansen and Nissenbaum 2009).

Realism is considered a useful framework by some for understanding cyberspace. As Reardon and Choucri (2012, 6) write: 'realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilising or destabilising, whether cyber technologies will be a new source of conflict or of peace, and whether states will engage in cyber arms racing.' The rest of this chapter considers specific realist-informed issues in cyberspace and evaluates their relevance.

Anarchy and Security Competition in Cyberspace

Anarchy is the fundamental assumption underlying structural realist theories and refers to the lack of overarching authority to police the international system which instils a sense of distrust among states (Waltz 1979). This forces states to rely on self-help measures to achieve security or pursue their interests. For defensive realists, much of the causes of conflict arise from the competition between security-seeking states. The security dilemma describes the phenomenon whereby 'many of the means by which a state tries to increase its security decrease the security of others' (Jervis 1978, 169). Actions such as military build-ups or alliance making are often perceived as threats by other states who then take similar measures to enhance their own security; this process is often termed the spiral model with each action forcing a reaction (Glaser 2004, 44). The spiral model is at the heart of traditional conceptualisations of an escalating arms race which are said to cause rapid shifts in the balance of power, an increase in international tension, and a greater risk of miscalculation and conflict (Richardson 1960; Vasquez 1993).

In many ways, anarchy and its effects describe cyberspace well. Liberal IR theorists argue that the dangerous effects of anarchy can be ameliorated by global institutions which mediate interstate disputes and reduce uncertainty through increased information (Russett and Oneal 2001, 163-4). However, the cyber domain lacks effective global institutional governance. Relevant organisations include the International Telecommunications Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN), but their functions and competencies do not extend to conflict management.

Media reports of a cyber arms race are frequent (Paletta et al. 2015; Corera 2015), and this increased militarisation of cyberspace is evident through the creation of new military organisations, the drafting of cyber-military doctrines, the increase in cyber security budgets, and the hiring of cyber 'warriors' (Craig and Valeriano 2016a). A more secretive development is the suggested stockpiling of malicious code which can be used as weapons (Rid and McBurney 2012). Furthermore, Craig and Valeriano (2016a) provide empirical evidence demonstrating a relationship between build-ups in cyber capabilities and mutual perceptions of threat and competition between states in a select number of cases.

Realism can help explain the source of cyber arms racing behaviour as a response to threat in an anarchic world. Jervis (1978, 187-194) notes that the security dilemma is at its most intense when a build-up in offensive capabilities is more cost-effective than a build-up in defensive capabilities. The security dilemma is also more severe when offensive and defensive capabilities are indistinguishable. If so, states are unable to signal benign intentions and any build up in capability will be seen as a potential threat (199-206). In cyberspace, capabilities are very difficult to distinguish. For one, it is impossible to verify the offensive zero day exploits governments possess since they are, by definition, unknown. Moreover, cyber military organisations like US Cyber Command tend to have both defensive and offensive roles and if they are said to be increasing their budgets or personnel it is not obvious whether an offensive or defensive investment is being made. This fuels uncertainty and competition between states as they seek security in cyberspace.

For some realists, arms races increase the likelihood of war (Jervis 1978, 188; Van Evera 1998, 13), yet for others, military build-ups are a necessary means of deterring a revisionist power (Glaser 2004). A critical question is therefore whether security competition will escalate to actual conflict. Previous scholarship has demonstrated a relationship between arms races and both militarised interstate disputes and war (Sample 1997; Gibler et al. 2005). The concern here is whether cyber arms races will lead to a similar outcome. As Lord and Sharp (2011, 29) argue: 'conflict in cyberspace is uniquely predisposed to escalation given uncertainties about what constitutes an act of war and the growing number of state and non-state actors seeking offensive capabilities.'

The empirical record, however, suggests that although cyber conflict is becoming more frequent, this increase correlates with low level disruption and espionage tactics rather than more destructive forms of cyber warfare (Jensen, Maness, and Valeriano 2016, 17). Moreover, the data shows that cyber disputes are very unlikely to spill over into the physical domains of warfare suggesting that, rather than escalation, the prevailing trend is one of restraint (Valeriano and Maness 2016). Rather than live up to the predictions of the realist-informed spiral model, states appear to avoid escalation into warfare and restraint appears to be the prevailing norm instead. It may be too early to tell whether escalation may become a future trend, but thirty years of digital conflict demonstrate a remarkable degree of self-restraint in that states have avoided outright destruction and violence in cyberspace.

Cyber Power

Power is central to realism because it can ensure the independence and survival of the state in a self-help environment (Mearsheimer 2006, 79-81). As Morgenthau (1948, 13) claims: 'whatever the ultimate aim of international politics, power is always the immediate aim.' Realists often equate power to the state's assets such as the natural resources, industrial capacity, military strength, and population a state possesses (Morgenthau 1948, 80-108). The distribution of such capabilities among states is considered to have significant implications for stability in the international system. For instance, a longstanding debate has been whether a multipolar, bipolar, or unipolar power configuration creates a more peaceful world (Mearsheimer 2006, 78-80).

Cyber power is defined by Nye (2011, 123) as 'the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain', and its potential to transform international relations has become a prominent debate. Although there is no theory of cyber power within the realist literature, realism offers a framework to think about the distribution of power between actors and how this relates to conflict.

A core assumption of realism is that states are the most powerful and therefore most important actors in international politics. The information revolution challenges the primacy of the state, however, due to the greater involvement of non-state actors threatening traditional power dynamics (Eriksson and Giacomello 2006, 229). Non-state actors are increasingly important in international relations as Nye's (1990, 160) theory of power diffusion argues, and this is especially true in the cyber domain in which individual criminals, organisations, and terrorist groups can take advantage of the accessibility of the internet to threaten the dominance of the state, and where private firms play a role, both as providers of security and as sources of vulnerability.

We should not overstate this issue though because states are still the most dominant actors when it comes to cyber conflict. Non-state actors and terrorists do play a role, but their tactics have generally been ineffective or used as cover for nation-states seeking to hide their actions (Valeriano and Maness 2015, 164-187). It appears that states remain ultimately best placed to leverage the tools of cyber warfare with resources to invest in the manpower, research and development, and education that are unlikely to be rivalled by non-state actors.

It is hypothesised that due to the relative low cost of entry into the cyber warfare domain, traditionally weaker states challenge stronger states and reconfigure the power distribution in the system (Lango 2016, 12). For example, much attention has been paid to North Korea's training of thousands of hackers (Mulrine 2015), China's Unit 61398, accused of continual cyber espionage campaigns against the United States (Mandiant 2013), and the increasing sophistication in Iran's cyber warfare tactics (Aitel 2015). Traditional power dynamics are also undermined by the paradoxical idea that the most technologically advanced countries are also the most dependent on digital infrastructure and thus the most vulnerable to a crippling cyber-attack (Kolet 2001, 282). On the other hand, Lindsay (2013) argues that only the technological superpowers possess the ability to develop the most sophisticated cyber weaponry which suggests the cyber domain's asymmetric nature may be overstated.

Realism also raises the question of whether cyber capabilities give states' coercive power, referring to the capacity to induce compellence to one's will through inflicting or threatening damage upon an enemy (Schelling 1966, 1-34). There are serious doubts about the efficacy of cyber coercion, however, since the technology lacks the destructiveness of conventional military operations and is less likely to be taken seriously by the target state. Gartzke (2013, 2) highlights the limitations of internet-based warfare writing that: 'It is one thing for an opponent to idle a country's infrastructure, communications or military capabilities. It is quite another to ensure that the damage inflicted translates into a lasting shift in the balance of national capabilities or resolve.' He suggests that cyber weapons can only be effective when used simultaneously with conventional military operations. This argument has found empirical support in a statistical study on the effectiveness of different cyber offensive methods. Jensen, Valeriano, and Maness (2016) analyse data on cyber incidents between rival states and find that coercive cyber actions aimed at changing the behaviour of the target are generally ineffective compared with smaller scale disruption or espionage. These findings suggest that traditional notions of power and war do not necessarily translate well to the cyber domain, and that cyber power is not transformative of international politics.

The Cyber Offensive

The idea that attacking is cheaper, easier, more effective, and therefore a more prevalent strategy than defending features prominently in the cyber security discourse (Lieber 2014). This is based on the offense-defence balance theory which is used by defensive realists to explain why status quo powers are sometimes incentivised to go to war, postulating that when the prevailing military technology favours offensive over defensive operations, the prospects for interstate conflict increase (Quester 1977, Jervis 1978, Lynn-Jones 1995, Van Evera 1998). The offense is dominant in the international system, as Jervis (1978, 187) explains, when 'it is easier to destroy the other's army and take its territory than it is to defend one's own', and defence is dominant when 'it is easier to protect and to hold than it is to move forward, destroy, and take.'

When the advantage lies with the attackers, status quo powers are given strong incentives to increase their offensive capabilities and seek expansion or else risk being attacked themselves (Jervis 1978, 187-194). Technological factors are considered to shape the offense-defence balance in various ways. For instance, mobility enhancing technologies are said to favour the attackers, whereas technologies that increase firepower make defending more effective (Glaser and Kaufmann 1998). The theory has been used to explain the onset or absence of war in history, such as World War I, where the revolution in small arms and artillery created a widespread, albeit mistaken, belief among European leaders in the 'cult of the offensive' that encouraged them to launch pre-emptive wars or risk being attacked themselves. In reality, technology heavily favoured the defence as trench warfare demonstrated (Van Evera 1984). The theory has been thoroughly criticised, however, for its flawed logic and lack of parsimony (Davis, Finel, and Goddard 1998). More critically, Gortzak et al. (2005) demonstrate the theory's lack of empirical support as an explanation for interstate conflict. They find that neither the actual nor perceived offense-defence balance is a statistically significant predictor of war or militarised interstate disputes, thus challenging the entire enterprise.

Despite the challenges, the theory has found a resurgent popularity in the cyber security debate. The cyber offense is widely assumed to be more effective than defence due to its relative ease and cheapness, the potential damage it could inflict on society, its instantaneous nature, and because attacks need only target a single vulnerability to succeed, whereas defence involves securing entire networks and patching vulnerabilities that the defender is unaware of before they have been exploited (Lieber 2014, 100-3). Libicki (2009, 32) claims that offensive capabilities are a more cost-effective investment in that 'another dollar's worth of offense requires far more than another dollar's worth of defence to restore prior levels of security'. Going further, Saltzman (2013, 43-4) reconceptualises the offense-defence theory to fit the non-territorial nature of cyber technologies with 'versatility' and 'byte-power' replacing mobility and firepower as the key determinants of the offense dominance of cyberspace.

There are two important reasons to argue that these claims are overstated. Real-world cases can help demonstrate that, first, the utilisation of cyber weapons is not as easy or cheap as is often assumed, therefore casting doubt on one of the main determinants of the offense-defence balance, and second, that the utility of cyber weapons as a coercive tool of warfare is likely overstated, suggesting that offensive cyber operations are not necessarily advantageous.

Rather than being an easy operation, the 'Stuxnet' virus, that was developed and implemented by the United States and Israel and discovered in the networks of an Iranian nuclear power facility in 2010, was, according to experts, a complex operation that took several years to develop, costing as much as $300 million, and which likely required a human operative (Valeriano and Maness 2015, 151). The incident, which had intended to hold back Iran's enrichment of nuclear material, destroyed one fifth of the facility's centrifuges (Sanger 2012, 205). However, the rate of enrichment actually increased during this episode, highlighting the limited impact of even the most advanced of offensive cyber actions (Lindsay 2013, 391).

Similar conclusions can be drawn from the December 2015 hack of the Ukrainian power grid which caused a blackout for over 230,000 residents in Western Ukraine. The incident involved Russian hackers disabling power supplies and launching a telephone denial of service attack against customer service call centres to prevent responses to the outages. Far from being an easy operation, the logistics and months of preparation involved were considered 'highly sophisticated' (Zetter 2016). The attack was also clearly limited in its impact on the target in that power was quickly restored, due to a manual override system. These prominent incidents suggest that offensive cyber operations are neither cheap, easy, nor effective in achieving strategic victory.

In line with the predictions made by the offense-defence balance hypothesis, even if we grant that the cyber domain is offense dominant, or at least perceived to be, then it begs the question of why we haven't witnessed a greater incidence of cyber conflict. The empirical record shows, to the contrary, that between 2001 and 2011, only 20 out of 126 rival pairs of states engaged in cyber conflict which has mostly occurred at low levels of severity (Valeriano and Maness 2014, 1). The usage of cyber weapons, therefore, does not appear to be determined by the supposed offensive nature of cyber technology. Given current realities, the offense-defence balance theory is unlikely to be useful in predicting cyber conflict. What is more dangerous is if policy makers shape their policies around assumptions of offense-dominance, build-up offensive capabilities, and risk destabilising the cyber domain.

Cyber Deterrence

For realists, the acquisition of military capabilities is key to deterring aggression from other states and maintaining national security (Morgenthau 1947, 14). Deterrence aims at discouraging attacks through a demonstration of one's military capacity and willingness to respond in kind. Deterrence theory rose to prominence during the Cold War because of the threat of mutually assured destruction from nuclear weapons, and realists figure prominently in the debate arguing that nuclear weapons have a stabilising effect on international relations (Waltz 1990; Mearsheimer 1990, 19-20). Deterrence logic now appears to be influencing cyber policy. For example, in its national cyber security strategy, the US government policy is aimed at 'convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States' (Department of Defense 2015), and the UK government, too, has spoken explicitly about the need to respond to cyber incidents with offensive actions (Elgot 2016).

Although it may seem an attractive option because of the perceived difficulty of defence as discussed earlier, there are several issues that undermine cyber deterrence. First, a state's ability to retaliate is not physically demonstrable due to the virtual nature of cyber weapons and the secrecy states maintain over them. Second, unlike nuclear weapons, cyber weapons do not have the same destructive capacity and so, to have a sufficient deterrent effect, would have to be used repeatedly and to great effect. This is difficult, however, because each cyber weapon is designed for a specific vulnerability which could be subsequently patched. Third, attributing the source of cyber incidents can be difficult and perpetrators often deny involvement. In such cases, therefore, a state cannot be certain of whom to respond against (Libicki 2009, 39-73). These arguments suggest that deterring aggression through cyber means is an unworkable policy in practice.

Considering the difficulties of deterrence when restricted to the cyber domain, moving towards a more inclusive idea of cross domain deterrence may offer a way forward (Gartzke and Lindsay 2014). It is also a concerning point that, while appreciating the inherent difficulties in protecting networks, governments may not be prioritising defensive measures (Rid 2013, 173; McGraw 2013, 110; Craig and Valeriano 2016b). Critical infrastructure often remains undefended, or reliant on older technology. It has been reported, for instance, that the Department of Homeland Security's EINSTEIN intrusion detection system has failed to detect 94% of the most common types of vulnerabilities (Sternstein 2016). Deterrence as a theory depends on the ability of the target state to survive a first strike, and this nuance is lost in discussions of cyber deterrence.

Another concern is the lack of discussion of the sources of discontent between entities that would lead to conflict in the first place. Given that much cyber conflict takes place between historically rival states (Valeriano and Maness 2014), often over territorial issues, perhaps working towards the settlement of outstanding issues of contention between actors ought to be given greater priority over nebulous and indemonstrable threats of retaliation.

Conclusion

As a theory mostly concerned with issues of national security and power, realism would appear to be the instinctive international relations perspective for understanding cyber conflict. Our analysis suggests that realism does remain a relevant framework for identifying important security-related issues in the cyber domain and can sometimes provide useful insights about some enduring characteristics of international relations. However, realist theories about conflict often fall substantially short in explaining the unique dynamics of cyber conflict.

In many ways, the cyber domain resembles a realist world with its anarchical nature and lack of institutional governance where states fear one another and develop their capabilities in response. Yet, it is unclear whether cyber arms races are likely to escalate into cyber conflict. Realism also raises interesting questions about cyber power, about who possesses it, and how it relates to international stability. In terms of whether cyber power will transform traditional power dynamics, the evidence suggests this is not the case. The trend we have seen thus far has been restrained from full-blown cyber war in favour of less destructive forms of cyber interactions.

The offense-defence balance is the clearest example of a realist theory being used to explain the cyber domain, but it appears empirically inaccurate in its assumptions about the cyber domain and its predictions about cyber conflict. Real-world cases of cyber conflict suggest the offense is not as easy as is often assumed and the fact that we have not seen much cyber conflict suggest the theory is misplaced. Importing the notion of deterrence from the nuclear era is furthermore ill-judged and makes little sense in the context of the reality of cyber weapons.

Prudence, a foundation of classical realism, may offer the most viable policy advice. As Machiavelli notes, the Prince ‘should proceed moderately and with prudence and humanity, so that an excess of confidence may not make him incautious’ (Vasquez 1995, 17). Due to the uncertainty surrounding the use of cyber technology as an offensive weapon, states should proceed with caution in the cyber domain and focus on creating resilient defences. Indeed, by refraining from outright cyber war, many states have so far remained rather prudent in their behaviour in cyberspace and this is an outcome that realist theorists would find appealing and an area for further theoretical elaboration.

Given the issues raised here, we encourage the development of new theories based on empirical observation or the deductive logics of the cyber domain rather than automatically falling back on realist theories that were developed to explain kinetic forms of warfare. With further empirical research, we can gain more precise understandings of key issues such as the impact of cyber arms races on interstate relations, the distribution of cyber capabilities among state and non-state actors, and the reasons for restraint despite the intense security competition and perceptions of an offensive advantage. More precise answers to these questions can help us formulate better policy guidance for governments.

References

Aitel, Dave. 2015. “Iran is emerging as one of the most dangerous cyber threats to the US”. *Business Insider UK*, 2 December. http://uk.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-the-us-2015-12?r=US&IR=T

Arquilla, John and David Ronfeldt. 1993. “Cyberwar is Coming!”. *Comparative Strategy* 12(2): 141–65.

Bumiller, Elisabeth and Thom Shanker. 2012. “Panetta Warns of Dire Threat of Cyberattack on U.S.”.*The New York Times*, 11 October. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Cavelty, Myriam D. 2008. *Cyber-Security and Threat Politics: US efforts to secure the information age* . London: Routledge.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco.

Corera, Gordon. 2015. “Rapid escalation of the cyber-arms race”. *BBC News*, 29 April. http://www.bbc.co.uk/news/uk-32493516

Craig, Anthony J. S. and Brandon Valeriano. 2016a. “Conceptualising Cyber Arms Races.” IEEE Proceedings for CCDCOE CyberCon, 8th International Conference on Cyber Conflict: Cyber Power, 141–58.

Craig, Anthony J. S. and Brandon Valeriano. 2016b. “Reacting to Cyber Threats: Protection and Security in the Digital Era”. *Global Security and Intelligence Studies* 1(2): 21–41.

Davis, James W., Bernard I. Finel, and Stacie E. Goddard. 1998. “Correspondence: Taking Offense at Offense Defense Theory”. *International Security* 23(3): 179–206.

Department of Defense. 2015. “The DOD Cyber Strategy”. 17 April. http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Elgot, Jessica. 2016. “UK must build cyber-attack capability, chancellor says”. *The Guardian*, 1 November. https://www.theguardian.com/politics/2016/nov/01/uk-must-build-cyber-attack-capability-chancellor-says-cybersecurity

Eriksson, Johan and Giampiero Giacomello. 2006. “The Information Revolution, Security, and International

Relations: (IR) Relevant Theory?”. *International Political Science Review* 27(3): 221–44.

Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth”. *International Security* 38(2): 41–73.

Gibler, Douglas M., Toby J. Rider, and Marc L. Hutchison. 2005. “Taking Arms Against a Sea of Troubles: Conventional Arms Races During Periods of Rivalry”. *Journal of Peace Research* 42(2): 131–47.

Glaser, Charles L. 2004. “When Are Arms Races Dangerous? Rational versus Suboptimal Arming”. *International Security* 28(4): 44–84.

Glaser, Charles L., and Chaim Kaufmann. 1998. “What is the offense-defense balance and can we measure it?”. *International Security* 22(4): 44–82.

Gortzak, Yoav, Yoram Z. Haftel, and Kevin Sweeney. 2005. “Offense-Defense Theory: An Empirical Assessment”. *Journal of Conflict Resolution* 49(1): 67–89.

Hansen, Lene and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School”. *International Studies Quarterly* 53: 1155–75.

Jensen, Benjamin, Ryan C. Maness, and Brandon Valeriano. 2016. “Cyber Victory: The Efficacy of Cyber Power”. Unpublished Manuscript.

Jervis, Robert. 1978. “Cooperation Under the Security Dilemma”. *World Politics* 30(2): 167–214.

Kolet, Kristin S. 2001. “Asymmetric Threats to the United States”. *Comparative Strategy* 20(3): 277–92.

Lord, Kristin M. and Travis Sharp. 2011. “America’s Cyber Future: Security and Prosperity in the Information Age”. *Center for a New American Security,* 1: 1–62. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf

Lango, Hans-Inge. 2016. “Competing Academic Approaches to Cyber Security”. *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*, edited by Karsten Friis and Jens Ringsmose, 7-26. London: Routledge.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Lieber, Kier. 2014. “The Offense-Defense Balance and Cyber Warfare”. *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla. Monterey, California: Naval Postgraduate School.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare”. *Security Studies* 22(3): 365–404.

Lindsay, Jon R. and Erik Gartzke. 2016. “Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept”. *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Erik Gartzke and Jon R. Lindsay. La Jolla, CA: Manuscript.

Lynn-Jones, Sean M. 1995. “Offense-Defense Theory and its Critics”. *Security Studies* 4(4): 660–91.

Mandiant. 2013. “Exposing One of China’s Cyber Espionage Units”. 19 February. (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, Accessed 06/05/2017)

McCarthy, Justin. 2016. “Americans Cite Cyberterrorism Among Top Three Threats to U.S.”. *Gallup*, 10 February. http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx

McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security In)". *Journal of Strategic Studies* 36(1): 109–19.

Mearsheimer, John J. 1990. "Back to the Future: Instability in Europe After the Cold War". *International* Security 15(1): 5–56.

Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.

Mearsheimer, John J. 2006. "Structural Realism". *International Relations Theories: Discipline and Diversity*, edited by Tim Dunne, Milja Kurki, and Steve Smith, 71-88. Oxford: Oxford University Press.

Morgenthau, Hans J. 1948. *Politics among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf.

Mulrine, Anna. 2016. "How North Korea built up a cadre of code warriors prepared for cyberwar".*Christian Science Monitor*, 6 February. http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-a-cadre-of-code-warriors-prepared-for-cyberwar

Nye, Joseph S. 1990. "Soft Power". *Foreign Policy* 80: 153–71.

Nye, Joseph S. 2011. *The Future of Power*. New York: Public Affairs.

Paletta, Damien, Danny Yadron, and Jennifer Valentino-Devries. 2015. "Cyberwar Ignites a New Arms Race".*Wall Street Journal*, 11 October. http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128

Quester, George H. 1977. *Offence and Defence in the International System*. New York: John Wiley and Sons.

Reardon, Robert, and Nazli Choucri. 2012. "The Role of Cyberspace in International Relations: A View of the Literature". Paper presented at the 2012 ISA Annual Convention, San Diego, CA. 1 April.

Richardson, Lewis F. 1960. *Arms and Insecurity: A Mathematical Study of the Causes and Origins of War* , edited by Nicolas Rashevsky and Ernesto Trucco. Pittsburgh: The Boxwood Press.

Rid, Thomas, and Peter McBurney. 2012. "Cyber-Weapons". *The RUSI Journal* 157(1): 6–13.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. C Hurst & Co Publishers Ltd.

Ripsman, Norrin M., Jeffrey W. Taliaferro, and Steven E. Lobell. 2016.*Neoclassical Realist Theory of International Politics*. New York: Oxford University Press.

Rosecrance, Richard, and Arthur Stein. 1993. *The Domestic Bases of Grand Strategy*. Ithaca: Cornell University Press.

Russett, Bruce and Jon ONeal. 2001. *Triangulating Peace: Democracy, Interdependence, and International Organizations*. New York: W. W. Norton & Company.

Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance". *Contemporary Security Policy* 34: 40–63.

Sample, Susan G. 1997. "Arms Race and Dispute Escalation: Resolving the Debate". *Journal of Peace Research* 31(1): 7–22.

Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* . New York: Random House.

Schelling, Thomas C. 1966. *Arms and Influence*. Yale University Press.

Schmidt, Brian C. 2002. "On the History and Historiography of International Relations". In*Handbook of International Relations,* edited by Walter Carlsnaes, Thomas Risse, and Beth A. Simmons, 3-22. London: Sage Publications.

Schroeder, Paul W. 1994. "Historical Reality vs. Neo-realist Theory". *International Security* 19(1): 108–48.

Senese, Paul D. and John A. Vasquez. 2008. *The Steps to War: An Empirical Study*. Princeton University Press.

Sternstein, A. 2016. "US Homeland Security's $6B Firewall Has More Than a Few Frightening Blind Spots"*Defense One*, 29 January. (http://www.defenseone.com/technology/2016/01/us-homeland-securitys-6b-firewall-has-more-few-frightening-blind-spots/125528/?oref=DefenseOneFB, Accessed 06/06/2017)

The Economist. 2010. "War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?". 1 July. (http://www.economist.com/node/16478792, accessed 06/06/2017)

Valeriano, Brandon and Ryan C. Maness. 2014. "The dynamics of cyber conflict between rival antagonists, 2001-11". *Journal of Peace Research* 51(3): 347–60.

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.

Valeriano, Brandon and Ryan C. Maness. 2016. "Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?". *Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives,* edited by Jens Ringsmore and Karsten Friis, 45-64. London: Routledge.

Van Evera, Stephen. 1984. "The Cult of the Offensive and the Origins of the First World War". *International Security* 9(1): 58–107.

Van Evera, Stephen. 1998. "Offense, Defense, and the Causes of War". *International Security* 22(4): 5–43.

Vasquez, John A. 1993. *The War Puzzle*. Cambridge: Cambridge University Press.

Vasquez, John A. 1995. *Classics of International Relations.* Pearson.

Vasquez, John. 1997. "The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition". *The American Political Science Review* 91(4):899–912.

Waltz, Kenneth N. 1979. *Theory of International Politics.* Addison-Wesley.

Waltz, Kenneth N. 1990. "Nuclear Myths and Political Realities". *American Political Science Review* 84(3): 731–45.

Zetter, Kim. 2016. "Inside the cunning, unprecedented hack of Ukraine's power grid". *Wired*. March 3. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

About the author:

Anthony J S Craig is a PhD candidate in the Department of Politics and International Relations at Cardiff University, and a member of the Research School on Peace and Conflict at the Peace Research Institute Oslo. His PhD

research investigates developments in national cyber capabilities across the international system.

Brandon Valeriano is the Donald Bren Chair of Armed Politics at the Marine Corps University and a Reader in the Department of Politics and International Relations at Cardiff University. He also serves as an adjunct fellow for the Niskanen Center. His two most recent books are *Cyber War versus Cyber Reality* at Oxford University Press (2015) and *Russia's Coercive Diplomacy* at Palgrave (2015).