Strategic Studies Quarterly

Power and Predation in Cyberspace

Christopher Whyte

Abstract

This article offers an alternative framework for understanding the sources of national security and power online. Wide-scale deployment of cyberweaponry regularly occurs beyond the scope of direct attacks on the infrastructure of national security and has a real effect on the power potential of states in the international system. Though the threat of cyberattack is a potent one, the greater impact on state power stems from the long-term disruption and distortion of the national innovation economy. The integration of civil and industrial functions with network systems allows for unprecedented levels of access to those second-order processes that underwrite national innovative potential and, ultimately, national power. A disruption to this underlying national apparatus via persistent, intrusive computer network exploitations (CNE) could diminish the innovative growth potential of sovereign actors in international affairs along several lines and essentially produce a power potential deficit that would not otherwise have existed.

✳ ✳ ✳ ✳ ✳

Can cyberweapons be used to alter the dynamics of global power? For many years, the answer to this question has been a resoundingly conditional one.[1] Certainly, the ubiquitous ability of state and nonstate actors alike to hack broadly with an ever-evolving set of digital tools offers support for the common notion that development of a significant and sophisticated digital establishment might benefit one or more global powers at the expense of others. The cyber domain—unlike the more traditional operating domains of sea, air, land, and space—offers actors the ability to affect and manipulate a man-made security environment defined wholly by the scope of those computer systems that are increas-

Christopher Whyte is a PhD candidate in the School of Policy, Government, and International Affairs at George Mason University. His research focuses on the intersection of technology, political behavior, and international security issues related to cybersecurity and the Asia-Pacific region. He is a WSD-Handa Fellow at Pacific Forum, Center for Strategic and International Studies, and has conducted research at several national security think tanks.

ingly at the heart of major socio-industrial processes. "Cyberweapons of mass destruction" that offer generic, far-reaching methods for shaping events in such environments could, in particular, supplement the abilities of geopolitical competitors as to affect a real change in the global balance of power.

However, the technical and organizational complexities involved in harnessing such processes on a large scale are significant. Although it seems fair to think broad-scoped digital weapons are likely to play an enabling role in any future conflict involving computer-assisted forces, the question of utility and lasting effect remains. If digital aggression is unable to cause lasting destruction or achieve permanent victories without a broader application of state capabilities, then could the capacity for launching massive cyberattacks really affect agent power in international affairs?[2]

Despite the emergence of a sizable body of analytic and technical work linking knowledge of network technologies to national security issues, attempts to explore this and related questions have been relatively unidimensional in considering the relationship between state power and cyberspace. Studies that focus on the nature of network-constituted capabilities as impactful in world affairs rarely stray from the idea of power diffusion. For instance, authors like Joseph Nye suggest that the unique meaning of network developments for power dynamics lies with the increased capacity of lesser actors.[3] Though useful for certain types of strategic analyses, this kind of assessment does little to speak to the broad-scoped nature of new technologies as increasingly synonymous with most mechanisms of social, commercial, and governmental capacity in the modern world. Cyberspace is not only an operational domain within which elements of the overt national security apparatus exist; it is also an avenue for access to national potential at a more fundamental level.

The purpose of this article is to develop a strategic understanding of the ways in which digital developments relate to creating and mobilizing power in both latent and societal terms. This is an alternative narrative of strategic power derived from network processes that rely on particular dynamics of interdependence and collective behavior at micro and macro levels. The central claim is that wide-scale deployment of cyberweaponry regularly occurs beyond the scope of direct attacks on the infrastructure of national security and has a real effect on the power potential of states in the international system. Though the threat of cyberattack is a potent one, the greater impact on state power stems from the long-term disruption and distortion of the national innovation economy.[4] Integrating civil and industrial functions with network systems allows unprecedented levels of access to those second-order processes that underwrite national innovative potential. Disrupting this underlying national apparatus via persistent, intrusive CNE, could diminish the innovative growth potential of sovereign actors in international affairs along several lines and essentially produce a power potential deficit that would not otherwise have existed.

The first consideration is the nature of cyberweaponry, noting the distinction between cyberweapons of mass destruction (CWMD) and mass effect (CWME). Next, the predator-prey model is used to describe the basic logic of interaction in international affairs and to explore the potential capacity-altering ability of CWME. Discussion centers on the implications of CWME deployment for state power, before looking at the incentives of involved agents. Another troubling reality—the inability to perfectly control such practices—is likely to interact with the incentives of different domestic actors to frustrate both governmental and intergovernmental efforts aimed at threat mitigation. This article concludes with a discussion of implications for governance and future research.

Cyberweaponry and Massive Effect

Why are cyberweapons generally considered to have the potential for massive effect and, thus, the potential to directly influence power dynamics? It is certainly the case that digital instruments lack a singular function. Unlike nuclear weapons, where the potential for massive strategic impact stems very clearly from the destructive potential of the bomb itself, the shape of digital methods of incursion and destruction depend very acutely on the technical environment in which they are deployed. As such, the label of weapon of mass destruction might appear to be an inaccurate or, at the very least, an incomplete one. This is reflected in the policy making and operational environment in which the use of cyberweapons is made possible, with decision makers forced to consider the unique technical dynamics of a target environment in such a recurring fashion as to make the strategic value of a specific given digital tool inconsistent over time. Both evolutionary and revolutionary systems development constantly alters the operational nature of the particular challenges facing analysts and officials, with the result that policy often accommodates situation-specific cyberweapon deployments rather than massive ones.

Nevertheless, cyberweapons and any digital instrument of manipulation have clear utility for massive effect deployments. One rationale is that cyberattacks, regardless of the technical shape or the manner of delivery of the payload, can and might be targeted at network processes that control, regulate, or coordinate the function of massive or massively dispersed systems. Today, concepts of digital arsenals most common to punditry and scholarship consider CWMD in much the same way we think of nuclear weapons—as instruments of destruction or incursion operationally defined by the scope of the desired outcome.[5] An example of such a WMD-style cyberattack would be the oft-cited threat of disruption to national power grids in which a vulnerability is exploited to shut down electrical networks across a nation.[6] Such an attack would lead to a widespread and far-reaching, disastrous outcome. Unsurprisingly, observers consider the types of payload needed to accomplish such an attack to be highly complex, technically sophisticated and deviously deployed at opportune times. One might say the same of nuclear or other WMD.

Another reason why we might consider cyberweapons to have massive effect potential has to do not with the scope of an intended outcome but rather with the scope of a given implemented incursion as one that is far-reaching.[7] Though an online arsenal that is deployed to achieve a massively destructive attack on, for example, an energy grid or nuclear facility is certainly of great concern, it is unquestionably the case that cyberweapons are increasingly deployed to undertake long-term, low-level sorties across a significant number of computer systems.[8] Generic code and design attributes, much like those found during analysis of the Stuxnet program, lend themselves to adaptive programs that are able to accomplish numerous incursive tasks, while simultaneously avoiding detection and spreading smartly. Though the particular nature of deployment was likely a response to the specific defenses in place in Iran's nuclear complex, Stuxnet stands as a good example of this type of assault, in which broadly-defined behavioral parameters guided remote action across a wide range of digital environments.[9] Beyond the physical sabotage of industrial facilities like Natanz, such generically coded, adaptable programs are also—and perhaps most often—found as spying assets or attempts to steal or corrupt valuable data.[10] Indeed, though CWME deployments are far less-closely linked to those major digital attacks that aim to overwhelm host systems, they are thought to constitute the bulk of aggressive cyber activities between countries around the world. Compared with the relatively small number of publicly reported, high-value attacks reported to have taken place against US entities in recent years, intellectual losses of more than $338 billion per year have been accrued from cyber incursions. This suggests that theft and distortion of information in its various forms are massively worthwhile pursuits.[11]

In sum, the extant literature on cyberspace and national security places a significant focus on the potential for massive digital attack on highly specific systems. In cybersecurity terms, "mass destruction" refers to the targeting of particular critical systems with sophisticated payloads at opportune moments. This is the main typology of behavior undertaken by opponents in cyberspace most closely tied by analytic and scholarly work to power political outcomes, perhaps because cyberweapons are thought of as enablers for broader geopolitical actions—like Russian operations in Georgia and Ukraine. In contrast, outside of confined circles, policy makers have broadly overlooked weapons of mass effect (WME) as having the potential for significant effects on power dynamics in international affairs, despite the relatively more common employment of such weapons. Of course, there is a difference between cyberattack and cyberexploitation, but semantic differentiation is made at the functional rather than the strategic level of policy planning.

This analytic disregard is problematic. Scholars and policy makers require a fuller understanding of the effects of cyberweaponry on power politics in international affairs at the micro and macro levels, not least because professional study of such developments lends itself to a more discursive and, potentially, cooperative international arena. The distinction is an important one, because CWME more intimately reflects the massive scope of network integration in relation to state functionality at every level of national security. Using the predator-prey model offers a first step in understanding the effects of those low-level, wide-effect instruments of interaction that are less easily categorized as amenable to mass destruction.

Predators and Prey in Cyberspace

How might observers best understand the affect, if any, of deployed CWME on power dynamics in international affairs? As previously noted, cyberspace remains remarkably unidimensional in the context of power in international systems. Nye and various others have regularly cited the greater relative abilities that digital capabilities award to relatively weaker, smaller actors in international affairs.[12] This idea of power diffusion simultaneously broadens and constrains the scope of debate on the subject of network technologies in saying that cyberspace is both a medium through which many actors can affect societal, economic, or security processes and an operating domain that has noteworthy limitations on possibilities for interaction and effect. It also inappropriately focuses debate concerning cyber capabilities on assessments of the character of governments, rather than on the strategic nature of the security environment. What do advancing network developments mean for different types of actors online? How might states adapt policies to deal with a proliferation of online threats from multiple vectors?

While, at the organizational level such questions are ultimately necessary, there is a need to revisit and consider questions of interaction in cyberspace if we are to construct an appropriate framework for fully understanding power dynamics and potentialities in the context of cyberweapons. Beyond one-time attacks on state infrastructure, broad-scoped network exploitations produce real long-term, value-added outcomes for aggressors online. This is particularly true when institutionally organized by an established authority. Theft of sensitive data endangers military preparedness and diminishes gaps between security competitors in political affairs. Moreover, theft of intellectual property and operational data on a massive scale curtails national potential as derived from a state's innovation infrastructure processes. In addition to the relatively intangible consequence of reduced soft power in the international system, theft reduces access to the various resources a country like the United States might call on as leverage to guarantee particular actions or more generally to underwrite credibility in political interactions. In short, the deployment of CWME portends considerable potential to reduce the power of vulnerable actors to extend power in a diplomatically coercive, institutional, and normative manner in the long term.

Commonly referenced in the natural sciences, the predator-prey model illustrates the potential effects of CWME on power dynamics in the international system. Though a strict read of the model is not apt for broad analysis, it is useful as an example of the manner in which actors interact in a system where there exists a degree of dependence on performance and resources and where awareness occupies an important part of the calculus undertaken by decision makers. It is important to realize that the treatment of CWMEs on power dynamics is not an intrinsically pessimistic one, even though the prospect of long-term structural repositioning might suggest so. As with any assessable threat to national and international security dynamics, rational outcomes merely define the scope of possibility and allow actors to consider the operational environment with a degree of contextual comprehension.

Relativity and Process in International Affairs

In world politics, actors at every level operate in a relative context. However, the metaphor is incomplete, as no actor can be assumed entirely predatory in nature nor can the complexities of the international system be described so simplistically. We might consider the lessons of the Lotka-Volterra model of interdependent predator and prey populations as exemplary of the relational nature of power.[13] When prospects are dependent upon the position of others, the ability to influence the strategic environment of a given system emerges from a combination of relative power differentials. If one considers the ever-increasing manner in which international political and security outcomes manifest as a function of various interdependent processes, there is little doubt the competitive behavior of one actor affects others to greater or lesser degrees. Indeed, this assumption is a staple of vast subfields of literature in political science and elsewhere.

As in the Lotka-Volterra model, interaction and abilities are functions of power as derived from second-order processes. Specific institutional power is the relative ability of an actor or population to survive and thrive. Rather than treat institutional power as the ability of some actors to defeat or significantly influence others through the extension of hard forces, such power is constrained in the long term via reference to the relative increase of each population. The birthrate of the predator group falls when there is overextension and a limited ability to survive off a reduced prey population. The birthrate of the prey group then rises again over time as predators experience slow population growth and lack the capacity to hunt effectively. Allowing for a certain broad degree of balance in the population levels in a set system (i.e., not considering instances of mass importation of new actors, etc.), this leads to a cyclical rise and fall in the relative prospects of the two actors.

How does this relate to an understanding of international relations useful to our analysis of CWME? The "refresh rate" denoted by birthrates in the Lotka-Volterra model reflects an assessment of relative strategic power and long-term power potential that is a common characteristic of policy practices in the history of realpolitik and major international conflict. In particular, the rise of Nazi Germany and the development of war plans in the 1930s are notable in that the role of latent power potential played an over-weighted role in influencing thinking on policy execution. The assessment of Adolf Hitler and much of the military leadership in Germany was that the Soviet Union (USSR), long considered to be the most immediate threat to German stability and prospects in a given conflict, would be increasingly difficult to combat.[14] Indeed, several historical studies have shown that Hitler believed the USSR—rapidly recovering from its civil wars and the horror of Joseph Stalin's early reign—would have effectively improved its refresh rate of power production so as to be relatively unassailable by 1950.[15] This accelerated war-planning efforts and likely influenced the development of a France-first policy married with a showpiece nonaggression pact. At the same time, Hitler and other Nazi leaders rarely missed an opportunity to express their view that, though the USSR was a more immediate challenge, the long-term competition for global hegemony would be one against the United States—a nation whose massive latent industrial potential later prompted Winston Churchill to utter the words "so we have won after all," upon hearing of the attack on Pearl Harbor.[16]

Thus, process-based, institutional power significantly underwrites the nature of systemic relationships and has historically had great influence on decision makers over time. Certainly, leaders and national security establishments necessarily premise many decisions on assessments of near-term threats to stability and prosperity. Moreover, incipient crises and the need to continually assess a changing operational environment—the latter a prominent characteristic of the diffuse, man-made cyber domain—incentivize the development of policies focused on a flexible ability to cope with emergent future challenges. But there is significant need to cast strategic operations in the context of the potential for changing dynamics. Long-term power differentials and potential capabilities in the future depend very much on the present behavior of actors, with the result that present policies must reflect a commitment to strategic positioning beyond the scope of immediate concerns.

Building Blocks of Power and Cyberspace as a Strategic Concern

Why consider the rise of CWME in the context of such institutional drivers of national power? In a nutshell, the notion of power as an institutional and developmental phenomenon is highly relevant to any discussion of cybersecurity and broader international security strategies in today's complex, globalized world because CWME are essentially designed as weapons of national sabotage. While the threat of deployed CWMD prompts consideration of various types of actions that must be undertaken to protect the integrity of national infrastructure and of military forces, CWME deployed on a large scale and able to flexibly utilize generically-designed digital tools have real value-diminishing effects on the power potential of different actors in the international system.

History bears out the fact that a state's geopolitical power and influence significantly comes from its ability to tailor economic processes toward national interests, and superior abilities to react and adapt in the international environment are largely derived from an ability to successfully cultivate an edge in innovative capabilities. In addition to common arguments that cite technological innovation as crucial in awarding certain states distinct hard-power advantages from revolutionary military capabilities, the postwar economics literature on national production and growth further pegs innovative capacity as a singularly important driver of market prosperity.[17] In more than just allowing for economic growth, a country's refresh rate determines the ability of a country to fuel future growth and maintain an innovative edge in global affairs. New intellectual property allows an increasingly unfettered ability to translate growth revenues into a more effective marketplace for the generation of robust intellectual, technological, and service-oriented products. Thus, in addition to an improved ability to produce powerful instruments of international operation, the better a nation is able to incentivize innovative growth, the better it is able to underwrite a future ability to offset static material outgrowths of foreign power. American hegemony in all things economic and security-related for the past seven decades is a reflection of this actualization of a structural ability to efficiently and effectively leverage innovative potential to perpetuate an advantageous systemic position.

CWME that aim to steal or disrupt information, particularly intellectual property and operational specifics, dramatically offset the ability of a nation or bloc to leverage an innovative edge in international competitions. This is particularly the case if broad-scoped CWME are periodically deployed in incapacitation attacks to provide additional disruption to the regular processes of targeted institutions. Victim companies and other organizations are then forced to compete on a playing field increasingly chosen and manipulated by advantaged opponents, regardless of the original source of innovative potential. For victims, this portends a development spiral increasingly defined by potential and periodically actualized threats and a necessary counteroperation that itself distorts innovation potential. In some situations, as in the process of selling massive product lines or in maintaining technological advantages in particular exchanges, this has significant immediate value. Over time, this can produce industry- and market-wide ripple effects, as lost revenue fails to yield the returns needed for continued innovative development in the future.

Of course, in the broader context of prospects for success in international interactions, such value-diminishing actions undertaken on a wide scale curtail and constrain the ability of an actor to wield hard, economic, and soft power by reducing the assets available for the purpose of underwriting geopolitical gestures. Military development necessarily suffers from the reduced innovative potential of a struggling private sector and production efforts become less of a cutting edge approach as new projects reflect increasingly reactionary considerations. Additionally, the reduction of a competitive edge for national companies diminishes prospects in international business and shrinks the degree to which a state can access foreign markets and influence foreign actors. This, in particular, has the effect of lessening the ability of a country to underwrite promises made for either coercive or mediative purposes; threats and assurances essentially become less credible as the power potential of an actor to follow through falls away.

Moreover, beyond the cumulative effects of CWME for the domestic polity, the use of broad-scoped digital instruments of intrusion to steal and disrupt information and processes portends opportunity cost advantages for aggressors. After all, innovation and successful sectoral operation are not without significant costs. Thus, stolen power potential from CWME deployment comes in the form of value-diminished investment for the victim nation/company and operational savings for an aggressor. Certainly, absorption and adaptation effectiveness diminish an aggressor's ability and benefit along these lines, but the potential is clear. Moreover, an aggressor might use the disruptive or information extraction capabilities provided by widely-deployed CWME to insulate itself from the significant uncertainties involved in investing to develop powerful national instruments for geopolitical influence. Avoiding the trial-and-error usually involved in the construction of both an effective national security apparatus and a strong private marketplace allows for programs that build on the earned successes of foreign actors and frees up funding for other national concerns, like social spending, military growth, or support for national economic development. Indeed, recent reports on the economic costs of cybercrime and espionage point to this fact—in essence a value-multiplier effect—as evidence of the gravity of major industry losses from digital attacks that otherwise might be pegged at no more than 2 percent of national income.[18] The benefits of a dollar stolen are thought to outweigh the gains of a dollar invested in research by as much as a factor of two.[19] And this multiplier effect has only been quantifiably considered in the aggregate; the explicit targeting of pivotal nuggets of intellectual capital might produce even greater advantages for aggressors.[20]

In sum, the spoils of nondestructive hacking could disproportionately sustain the ability of states, including potentially revisionist ones, to devote significant resources to areas of national interest. Though cyberspace is often considered to be its own operational domain, the fact of the matter is that networks intersect with societal processes at every level. Thus, beyond the use of digital pathways to mount destructive campaigns against actors in international affairs, broad-scoped instruments of intrusion and low-level systems assault are likely to have a real and measurable effect on the latent and institutional power available to states out into the future. Though power potential might appear as a diffuse variable relative to the immediate capabilities-based concerns most commonly considered by policy makers, cyberweapons present a strategic concern that is difficult to decouple from broader considerations of power and competition in international affairs. This is unavoidably so, because the integration of network technologies with core and peripheral socioeconomic functions continues.

Governance and the Payoffs of CWME Deployment

Since cyberweapons are developed and deployed diffusely in international society (i.e., not exclusively by states), it becomes important to ask if an appropriately concentrated effort to undermine foreign actors is a plausible strategic concern to be considered by policy makers. Answering this question requires a closer exploration of the incentives involved in developing and maintaining CWME arsenals and consideration of the positions of those agents—namely parochial organizations and government entities—whose actions might cumulatively constitute a regime.

An appropriate starting point for such an effort is also an odd one: the idea that centralized state manufacture and maintenance of aggressive CWME deployments cannot be assumed. The reason for this is simple: many incursive or predatory cyber campaigns are undertaken by private organizational or individual actors acting to better narrow interests. In most cases, central governments have appeared to lack the capacity to organize private society along such lines. Though relative gains produced by such efforts may ultimately benefit national processes and undergird national prospects for greater influence in world affairs, it is shortsighted to think that such a subversive and broadly diffuse regime is synonymous with policy at the highest level of strategic planning and decision making. Even in cases where this seems to be the case, the complexities involved in integrating multifunctional digital technologies across societies and government establishments suggests that any assumption of universality or adherence to centralized approaches is limited.

Given this, from where might potential support for established use of CWME on a national scale come? Can we expect such processes to be governed at all? At the most basic level, of course, development and utilization of offensive low-level digital techniques might originate wholly within the realm of private civil and industrial society. The ability of relatively weak actors and individuals to hack effectively and with little chance of getting caught alters the payoff structure involved in producing outcomes via illicit, rather than legitimate, means. Moreover, direct outside intrusion into agent concerns or knowledge of the strong possibility thereof can further tip the balance in favor of preemptively producing a CWME capability, as can the probable difficulties involved in seeking reparation for technically complex attacks through legitimate channels. In simple terms, potential gains and knowledge of possible hard-to-attribute competitor defection portends equilibrium where preemption is rational.

It is also plausible that governmental efforts might drive such a regime in two different ways. First, governments might recognize the potential for national gains and construct explicit, if well classified, regimes for directing such efforts. This may be significantly more likely for countries where government controls extend effectively into industry and civil society. Indeed, various reports attribute the high-level linkages involved in China's military, government, and bureaucratic establishments as beneficial for implementing high-level policy initiatives on cybersecurity on a broad scale.[21]

Second, it is possible that governance of this diffuse, massive process of widespread incentive to seek advantage online occurs itself in a diffuse and self-interested manner. Though governments tend to adopt broad positions of balanced regulation in line with strategic and national interests, it is commonly the case that sectoral operation is dictated by the relationship between governmental subentities and private/civil sector actors. Organizations, like the Department of Commerce, are significantly incentivized to support private sector operations within the context of enumerated policy interests defined much more broadly than a particular strategic stance on an issue might be. Likewise, particular subsections of the political elite are motivated to support local and regional economic interests, while national security bodies with narrow charters inevitably find direct and tacit support for private actor-instigated CWME deployments fall in line with operating imperatives not bounded by the presence of a high-level strategic directive on such operations. Governance, in short, can occur as a sequential result of a distributed series of compensatory payoff structures. This proposition is perhaps far more valuable by itself than the broader prospect of state-led CWME initiatives. The incentive-based emergence of such a regime merely requires some degree of diminished high-level control to play a role in motivating broad-scoped CWME intrusions.

Implications for Governance and Future Research

The problem of CWME and the long-term potential for dynamic power shifts as a strategic concern suffers as much from distributed governance issues as it does from the diffuse nature of the online environment. Affecting the regulatory control necessary for ensuring reductions in the development and deployment of CWME is likely to be as difficult as the challenging task of setting technical standards within which digital operators might simultaneously be protected and governed. Why? Quite simply, the incentive to hack is produced by the clear prospects for significant economic and circumstantial betterment that stem from CWME use. Moreover, motivation to hack is positively affected by the balance of attribution and other technological prospects that are likely to oscillate over time.

In the context of international cooperation and countermeasures that might be taken against the use of CWME, such difficulty in governing at home manifests in a significantly more foundational set of problems. Though greater cooperation for control of such regimes might be an obvious and desirable outcome, real progress is likely to face multitiered challenges on a recurring basis. First, as is often the case in international relations, verification of implementation of agreed frameworks and actions can be difficult when dealing with such a broad-scoped developmental issue. Governments are naturally secretive, and cyberspace is an area in which, due to the relatively ungoverned condition of public networks, programs and interests are closely guarded at the level of agencies. Second, in many cases, the gap between government policy making at the highest level and the instigation of new development or deployment of CWMEs at the level of substate actors can be immense. Trust in agreed frameworks or cooperative treaties would not only require credibility of process at the level of foreign government policy but also credibility of control over actors in those sectors of civil and industrial society that are, in addition to military or intelligence agencies, the real targets of any action. This may be problematic even in the case of government units, as national security outfits resist the constraints of narrow parameters for action and others argue for tight regulation to protect parochial interests. Finally, cooperation on this particular typology of cyberweapons—whether the particular circumstances describe cases of cyberespionage, cybercrime, or otherwise—is likely to require recurring review and an approach that emphasizes the need to alter framework procedures. After all, any success in regulating the deployment of such value-adding instruments will come into constant conflict with the inherent payoff motivations of continued development. The potential payoffs of such low-end, high-gains cyber efforts represent a constant lure for government elements across a range of functions, again suggesting that broad-scoped cooperation is prone to defection.

So, how should policy makers approach the issue of CWME—as distinct from CWMD—and set about a diplomatic treatment of such a long-term challenge to national interests? Though further research may produce a more concise statement of policy recommendations moving forward, three clear angles of approach emerge. First, policy makers may find significantly more interest among foreign counterparts in cooperating on matters involving CWMEs that are generally considered to be unrelated to national power and process. These include incidents of cyber hacktivism by civil society groups distinct from oft-cited and accused examples of state incursion for political purpose, like North Korea's 2013 attack on South Korean television stations or Russian vandalism of Estonian political web sites in 2007. The hope for success here would be twofold. First, attempts to coordinate international antihacking efforts along narrowly-defined operational lines and boost multilateral observational capacities could constrain the relative ability of aggressive national agents to intrude without detection. Second, such an effort would aid in the development of international norms of behavior for low-level incursive activities in cyberspace, with the intended result of making coordinated condemnation of and action against broader CWMEs easier to achieve.

Second, policy makers and practitioners may find it easier to prosecute a campaign of counter-CWME development and deployment by focusing on those government and substate actors that have major reputational interests to consider. Multinational corporations, in particular, are likely prospects for any such regime, as the incentive to hack at any level contends with the need to maintain an ability to legitimately operate across multiple jurisdictions and within various markets.

Third, and perhaps most importantly, policy makers are likely to find progress more easily if broad cooperative efforts are underwritten and informed by an extensive and well-designed data collection and modeling program. Such a program could identify broader patterns in CWME activity (verified or suspected) and interact with data on national productive potential to produce quantifiable mechanisms for assessing CWME impacts, tipping points, and functionality. Such a program would be a first step in producing a national capability to effectively coordinate on diffuse issues of cybersecurity and underwrite deterrent, compellent, and diplomatic efforts in interactions within and across borders.

It is not enough, of course, to simply prescribe an effective data regime to undergird national security policy-making efforts without recognizing the clear challenges involved. In particular, the cybersecurity field of analysts, scholars, and practitioners faces both parametric and motivational problems requiring broader research that interlinks existing bodies of knowledge in political science, military studies, and technical fields with the developmental realities of digital developments.

On the one hand, theory must catch up in such a way that policy makers might be afforded the ability to link complex ground truths with generalizable "systems of parts" that can provide insights appropriate for grand strategy planning. Then again, questions of incentives and data access must be broached in such a way as to effectively render information to which conceptual frames might be applied. Suggested voluntary data collection programs are a good start.[22] However, future efforts will need to contend with major issues. Notably, data fitted to theoretically derived models must match program requirements if robust results are to be had. This suggests that policy and rhetoric must work toward the goal of making data volunteering compatible with the self-interests of private actors—a task made particularly difficult by the need to match market and structural imperatives with strategic ones. It is critical that skewed availability of data should not, as it has in the past, act to distort strategic planning by emphasizing knowable incremental threats at the expense of relatively inaccessible ones.

In the end, it is perhaps most important to note that the various challenges presented by the existence of deployable CWME that could have a real impact on systemic power differentials are not intrinsically negative for states around the world. The dynamics described above do not, in themselves, portend an enduring arms race in the digital world in which actors at every level of society are unerringly motivated to participate. Certainly, developmental incentives and structural realities complicate the ability of policy makers and statesmen to coordinate and produce peaceable solutions to such national security woes. However, a legitimate cyber regime that "reduce[s] transaction costs and uncertainty" and acts to perpetuate appropriate norms of cooperation and mutual restraint would do much to counteract the negative effects of potential threats.[23] The task ahead for practitioners, as much as it is technical in nature, is principally one of doing just that—transmuting the national benefits of such hacking and ensuring that cooperative certitude is a preferable option for self-interested actors in geopolitical affairs. For this to occur, fuller understanding of the parameters of cyber phenomena, the theoretical and technical, is needed.

Conclusion

Though cyberespionage and broad-scope intrusion make their way onto the pages of most cybersecurity literature and punditry these days, it is vital that we develop a strategic understanding of the potential costs and ramifications of sectoral and parochial behaviors as they apply at the highest level of international political considerations. The ramifications of doing so are more than just greater understanding of the evolution of the cyber phenomenon; they are a chance for better-constructed policy and the evolution of a more discursive environment for producing meaningful solutions to our most foundational security challenges. Significant research and data explication are needed in the future if analysts and scholars are to effectively reconcile questions of CWME and strategic initiative within the cyber ecosystem of states. The complexities involved in understanding the shape of competing market and institutional formats for organizing incursive actions portend much needed developments along several lines and speak to the evolution of the cyber field in security and political studies as one of multifaceted focus.

The arguments and suggestions made here are a first step toward expanding professional and scholarly thought along these lines. Key among the takeaways is the fact that low-level intrusion is not only possible; it is the norm for incursive interactions in cyberspace. CWME pose a threat to global power dynamics so distinctly different from more commonly considered digital instruments of sabotage that they require both separate consideration as a strategic artifact and a unique approach to professional and diplomatic engagement on the subject. Moreover, and perhaps more so than with "traditional" online national security concerns, CWME can be creatures of socioeconomic construction as easily as they are of defense establishments. Where strategies of CWMD prevention or deployment might require a concentrated series of complex efforts, the shape of CWME counterproliferation is likely to be one of broad state and institutional enterprise.

Notes

[1] For the most comprehensive survey of the development of a cybersecurity literature as a subfield of the international security field of study, *see* Robert Reardon and Nazli Choucri, “The Role of Cyberspace in International Relations: A View of the Literature” (paper, 2012 ISA Annual Convention, San Diego, CA, 1 April 2012), http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf.

[2] For a full summary of these arguments, *see* Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International Security* 38, no. 2 (Fall 2013): 41–73, http://www.mitpressjournals.org/doi/pdfplus/10.1162/ISEC_a_00136; and Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32, http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939.

[3] Joseph S. Nye, “Cyber Power” (paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

[4] Scholarship on cybersecurity and international security has yet to fully develop a narrative understanding of the interconnections between markets, institutions, and various national processes. However, recognition that the innovation economy—i.e., the dynamics of interaction between productivity, infrastructure, and knowledge inputs that drive economic outcomes and incentives—might be distorted by digital manipulations on a broad scale is not new. *See* James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, 22 July 2013), http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf. Nevertheless, linkages remain woefully understudied.

[5] This assumption is drawn from a number of recent works, perhaps the most notable of which is Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security* 38, no. 2 (Fall 2013): 7–40, http://belfercenter.ksg.harvard.edu/files/IS3802_pp007-040.pdf.

[6] For example, *see* James Adams, “Virtual Defense,” *Foreign Affairs* 80, no. 3 (May/June 2001): 98–112, http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense.

[7] This distinction is a notable takeaway from Ralph Langner’s cornerstone work on the development of Stuxnet and related uses of cyberweapons. For examples, *see* Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve* (Arlington, VA: Langner Group, November 2013), http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

[8] Ibid., 4.

[9] Ibid., 22. For a thorough account of the discovery and exploration of Stuxnet, *see* Kim Zetter, “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History,” *Wired: Threat Level Blog*, 11 July 2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet; and Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (2013): 365–404, http://www.tandfonline.com/doi/pdf/10.1080/09636412.2013.816122.

[10] For a good description of the use of such tools in offensive operations, *see* William A. Owens, Kenneth W. Dam, and Herbert S. Lin, ed., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009).

[11] *See* Executive Office of the President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House, 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. A 2013 Center for Strategic and International Studies and McAfee report estimates that, at time of production in July, annual costs to US persons and companies from cybercrime and espionage had run between $24 billion and $120 billion. *See* Lewis and Baker, *Economic Impact of Cybercrime and Cyber Espionage*, 5.

12. Nye, "Cyber Power;" Rid, "Cyber War Will Not Take Place;" and Mary Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54, no. 2 (June 2010): 381–401.

13. Reference to the predator-prey relationship is not uncommon in the natural sciences. Described by a series of equations developed by Alfred Lotka and Vitto Voltera in the early twentieth century, the relationship outlines the parameters of interaction and competition between two agents in a given system (usually given as wolves/foxes and rabbits). The basic assumption made in the model is that one agent (the wolves/foxes) is dependent on the other (rabbits) as a food source. This ties the prospects of both agents together by means of defining an environment of constrained resources. *See* Alfred J. Lotka, *Elements of Physical Biology* (Baltimore, MD: Williams & Wilkins Company, 1925); and Vito Volterra, *Variazioni e fluttuazioni del numero dindividui in specie animali conviventi* (Rome, Italy: Memoria Accademia dei Lincei, 1926), http://bpfe.eclap.eu/eclap/axmedis/b/bd0/00000-bd05ae74-d168-4c92-9a65-4f461377f7bd/2/~saved-on-db-bd05ae74-d168-4c92-9a65-4f461377f7bd.pdf.

14. Antony Beevor, *The Second World War*, 1st ed., (New York: Little, Brown and Company, 2012).

15. Ibid., 108.

16. Ibid., 289.

17. *See* Moses Abramovitz, *Resource and Output Trends in the United States Since 1870* (Washington, DC: National Bureau of Economic Research, 1956), http://www.nber.org/chapters/c5650.pdf; and Robert M. Solow, "Technical Change and the Aggregate Production Function," *Review of Economics and Statistics* 39, no. 3 (August 1957): 312–20, http://faculty.georgetown.edu/mh5/class/econ489/Solow-Growth-Accounting.pdf.

18. *See* Lewis and Baker, *Economic Impact of Cybercrime and Cyber Espionage*, 15.

19. Ibid., 16.

20. Ibid., 17.

21. *See* U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: US Government Printing Office, November 2012), 147–51; U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress* (Washington, DC: US Government Printing Office, November 2013), 243–65; Jon Lindsay, *China and Cybersecurity: Political, Economic, and Strategic Dimensions* (workshops, University of California, San Diego, April 2012); and Bryan A. Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012), http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

22. *See* Karl Frederick Rauscher and Erin Nealy Cox, *Measuring the Cybersecurity Problem* (New York: East West Institute, 21 October 2013), http://issuu.com/ewipublications/docs/mcp_final_10_22_2013/4.

23. James Wood Forsyth Jr., "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no. 1 (Spring 2013): 93–113, http://www.au.af.mil/au/ssq/digital/pdf/spring_13/forsyth.pdf.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.