STRATEGIC INSIGHTS

Volume 10, Issue 1
Spring 2011

Cyber Security in International Relations

Articles

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategic Insights. Volume 10, Issue 1, Spring 2011	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Center on Contemporary Conflict,Department of National Security Affairs,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**76**	

STRATEGIC INSIGHTS

Volume 10, Issue 1 • Spring 2011

Strategic Insights is a quarterly online journal published by the Center on Contemporary Conflict, Department of National Security Affairs, Naval Postgraduate School in Monterey, California.

We publish scholarly articles as well as viewpoints that address issues of current interest to the makers and executors of US national security policy. We are particularly interested in articles addressing homeland security, WMD/WME proliferation, regional conflict, and the contemporary role of US security forces. The journal seeks articles that will make our readers think, generate discussion, and gain new insight into the challenges and opportunities confronting US policymakers and military operators. Views that run counter to the conventional wisdom or official US government policy are welcomed.

You can contact the editors at ccc@nps.edu.

About the Cover

The cover on this edition of *Strategic Insights* features part of a map designed in December 2010 by Paul Butler, an intern on Facebook's data infrastructure engineering team. Mr. Butler sampled ten million pairs of friends from Facebook and plotted lines based on the distance between their locations. The more friendships between a pair of cities, the brighter the lines. The end result is not data plotted across a map—rather, *the map is made from the data itself*. Based only on the online relationships between people, this map shows the outlines of continents and even some international boundaries, offering a glimpse of how international relations unfold both in cyberspace and physical reality.

You can see the full map and read more about how Mr. Butler created it at:
http://www.facebook.com/notes/facebook-engineering/visualizing-friendships/469716398919

Foreword

Richard Clarke

"As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare…it has become just as critical to military operations as land, sea, air, and space." These words, written by Deputy Secretary of Defense William Lynn last fall in *Foreign Affairs*, cemented the status of cyberspace as a domain of warfare like all others, and coincided nicely with US Cyber Command reaching its full operational capacity. Yet, suggestions of a strategy in the pages of this article and subsequent publications from Cyber Command and its four-star commander, Keith Alexander, belie the fundamental fact that the United States military, government, private sector, and citizenry are all seriously vulnerable to cyber attack and that we have no coherent plan to protect America. "Active defense," by which Cyber Command means going offensive first, is not a strategy that will protect this nation. If anything is clear, it is that we have a remarkably well-developed offensive capability, but no commensurately serious commitment to defense. There is neither a plan nor any capability to defend America's civilian infrastructure, from banking to telecoms to aviation. Perhaps the most important thing Americans can do to make us safer from cyber war is to discuss it, openly, in academic journals, to debate aspects of cyber war in Congress, and to educate the public and the world through mass media. Thus, this volume by the Naval Postgraduate School is an important step in improving our security as a nation.

Given the central importance of net-centric warfare to our current military doctrine, I fear that this lack of clear thinking with regards to defense in cyberspace leaves not only our military, but our society as a whole, highly vulnerable to cyber attack. It will not be the first time that initial adopters of a new military technology, overcome with inertia or overconfident in the weapons they love and consider supreme, fail to defend effectively against that which they have just created. Thus it was that while American Colonel Billy Mitchell was the first to recognize the capability of small aircraft to destroy battleships, it was the Japanese Imperial Navy that most effectively harnessed this knowledge and nearly defeated the Americans in the Pacific during World War II. Great Britain invented the modern tank and a French Colonel, Charles de Gaulle, developed the first tactics of rapid attack with massed tanks supported by air and artillery. However, it was the Germans that perfected the tank design during the interwar period and employed de Gaulle's tactics with horrific efficiency in what they referred to as blitzkrieg. I fear that we may be on the precipice of a similar situation in cyber war, one that may leave the American military hamstrung and the US civilian infrastructure shredded.

Unlike the conventional examples from history, however, the threat to the United States in cyberspace will very likely not come from an adversary developing superior offensive capabilities. Rather it will be from one who can most effectively exploit the inherently asymmetrical nature of cyber war. While the notion of asymmetry in warfare is as old as the profession itself, its implications have rarely been so great as they are when placed in the context of cyber. To confront the United States military in conventional terms is a losing proposition; no other military today can surpass its capabilities on a tactical or strategic level. Yet, the conventional supremacy of the Americans is predicated upon a highly vulnerable foundation, its complete reliance upon information technology. Computers and networks enable all elements of the defense apparatus to function. From units in the field to procurement officers to strategic planners, all communications pass through various computer networks. Navigational and weapons systems aboard planes and ships depend on highly

sophisticated networked hardware and software, to say nothing of the thousands of satellites that provide imagery of nearly every inch of the earth. While this high degree of networking has brought unprecedented levels of productivity and efficiency, they also expose the entire operation to serious vulnerabilities. From the insider threat, as demonstrated by the WikiLeaks incidents, to the attacks that compromised the classified SIPRNet, to the hacking of Secretary of Defense Robert Gates' personal computer, the examples of the vulnerabilities in cyberspace to our military abound. For this simple reason, the single most effective way to prevent units from communicating, procurements from taking place, or F-16s from properly acquiring targets, is to compromise chips and software in order to attack the network infrastructure and advanced weaponry of the net-centric giant.

Nevertheless, for all of the potentially devastating implications for the United States military in a cyber war, such a war is probably not imminent. What ought to be of far greater importance not only to the United States, but to all industrialized nations, are the consequences of the current pandemic of economic cyber espionage. Economic warfare, which takes the shape of espionage conducted on an industrial scale against private corporations in all sectors across the globe, is happening every day. Intellectual property, proprietary information, bid and financial data – anything that comprises competitive knowledge in the digital global economy – is a potential target. The risks associated with such large-scale intellectual property theft pose an existential threat to the foundations of a state's economic leadership, competitiveness, and well-being. In our inter-connected world mutual dependencies among states abound, and thus, it would be in the long-term interest of few states to seek conventional war that could easily disrupt the delicate architecture of the global village. However, as the global competition for economic primacy intensifies in a knowledge-based global competition, the value of intellectual property, from research and development to biotech formulas to engineering designs, will only increase. China, among other nations, is systematically stealing terabytes of data at low cost, financially and diplomatically, and passing that data to its own companies. Private firms, limited by finite resources and obligations to maximize profits, will always lose against state-backed hackers unbound by such concerns. Governments, in the interest of maintaining economic stability, must therefore protect private industry and start the process of establishing an arms control regime in cyberspace.

Arms control for cyber war is too often summarily dismissed with the question of attribution. Critics assert that if you cannot definitively determine who committed an attack, you cannot hold anyone accountable for violating an agreement. Definitely establishing the origin of cyber attacks is extremely difficult post facto, and in nearly all cases one only ends up with an educated guess. What the argument essentially says is that arms control in cyber war cannot work because it would be too hard to establish. This is a refrain that I encountered multiple times over the course of my career at the Pentagon, State Department, and White House. Whether it was conventional force reduction in Europe, nuclear weapons limitation and reduction with the Soviets, or international agreements on chemical and biological weapons, the initial reaction invoked, without fail, the "it's too hard" argument. Yet we did, after long negotiations, draw down troop levels in Europe, and limit and reduce the numbers of nuclear weapons in our arsenal and ban chemical and biological weapons. With persistence, there are solutions. A way around the attribution problem may be to include in an international agreement on cyber arms control an Obligation to Assist clause. Such a clause would require states party to share information on attacks as they were taking place, and would require that states cut off computers engaged in malicious activity, as confirmed by other parties and an international monitor. Such a convention obviates the attribution issue. The responsibility for malicious traffic rests with the state in which the malicious traffic originates, regardless of whether the actual attacker is located within its borders. I concede that this proposition is not perfect, but it

is perhaps the basis of a discussion that must begin now, because the risks are too grave and despite the associated difficulties, there is a great potential for good.

Given the gravity of the implications of activities in this new domain of war fighting, it is vital that our national strategy be comprehensive, serious, and reflective of an open and frank debate, not just within the corridors of the Pentagon, but with academia and the broader public. Though the new Defense Department documents may suggest otherwise, "active defense" and "going first" do not constitute such a strategy. Again, I find myself reminded of historical precedent. In the early days of nuclear strategy, the Pentagon refused to share information regarding policies governing the use of nuclear weapons with anyone, let alone university professors. Yet as it became clear that the military's plan to strike first with the entire nuclear arsenal was not an optimal strategy, civilian officials began to see the value of having academics like Bill Kauffman and Herman Khan dissect and analyze this all too important topic. Those whom Fred Kaplan has called "wizards of Armageddon" brought a much-needed critical eye to the nuclear strategy debate, and slowly backed the nation away from the dangers of a policy governed by a hair trigger. We need a similar debate today regarding cyber war. Should the US government keep secret its knowledge about software vulnerabilities that put the US economic infrastructure at risk? We do not know can who initiate cyber operations against a foreign entity, nor do we know how we would respond if we were the victims of a cyber attack. At what point would we respond kinetically? When does the response require presidential approval? These are but a small fraction of the number of critical, yet unanswered, questions about the national cyber strategy that need to be addressed. Fortunately, this journal and others like it are beginning to explore precisely these kinds of questions and analyze the issues associated with cyber war, work that will undoubtedly ultimately contribute to making us all safer.

Beyond the Rift in Cyber Strategy

A middle ground for the US military posture in cyberspace

Jean-Loup Samaan

Introduction

Over the last five years, interest in cyber-defense has grown in earnest, particularly after the cyberattacks against the Estonian government in spring of 2007, the discovery of the GhostNet network targeting the Dali Lama's diplomatic offices in 2009, and the Stuxnet worm's disruption of the Iranian nuclear program in 2010. As a result, the US government has made substantial moves in the last two years towards the institutionalization of cyber-defense:

- The appointment of Howard Schmidt as Cybersecurity Coordinator for the Obama Administration in December 2009;

- The implementation of a formal partnership in October 2010 between the Department of Homeland Security and the Department of Defense, which specifies the responsibilities of each organization;

- Finally, the creation of the US Cyber Command in May 2010, a joint organization including components from all military services (the Army Forces Cyber Command, the U.S. Navy Fleet Cyber Command, the 24th Air Force, the Marine Corps Forces Cyberspace Command).

Despite these bureaucratic efforts in the White House and in the interagency process, this article argues that there remains a lack of consensus in Washington, particularly within the Department of Defense, on threat assessment in cyberspace and its military implications. A stark intellectual rift between "alarmists" and "skeptics" still prevails. As a result, this elementary battle has led to dysfunction in the institutional response to cyber-threats and jeopardizes the implementation of an effective military posture in cyberspace. Consequently, we need to reassess the relevance of cyberspace as a distinct military domain.

To that end, this article aims for a middle ground between these opposing views, supporting the idea that cyberattacks are more than just a technical nuisance, but less than an existential threat to US national security. As of today, they remain a valuable, but not decisive, tool of military action. At the operational level, it means that cyberspace is not an independent domain. In other words, while warfare in the air is different from warfare on the sea, it is possible to have one without the other. But warfare in cyberspace must be accompanied by warfare in one of these other domains to lead to physical effects. As a result, this paper recommends a comprehensive integration of cyberattacks (which are precisely *not* autonomous cyberwarfare) into a joint analysis of military battles. Because pundits have been focusing on the broad geopolitical implications of cyberattacks, the strategic literature lacks a systematic and detailed campaign analysis of these acts. This joint analysis would frame cyberattacks as offensive or defensive military engagements in the process of a larger naval, air, or land campaign. Based on the findings of this research, cyberattacks should be considered a subset of an offensive, a means of *denial* rather than a means of *punishment*. They aim at attaining an intermediate goal for the attacker.

Consequently, as long as cyber operations are launched by actors with broader objectives than

exclusively dominating channels of communication, there is legitimate doubt over whether a cyberwar could occur without an extension to other traditional military domains.

As a necessary word of caution, this article explicitly excludes cases of cyber-espionage whose aim differs from cyberattacks: while the former tries to steal and exploit information from an enemy (eg, the daily attempts of intrusion into the servers of the Defense Department), the latter are defined here in strict military terms to directly or indirectly destroy or disrupt targeted infrastructures. In other words, cyberattacks should be narrowly considered at the battle level as a component of the forces used by the attacker.

This article has three sections. The first section assesses the fundamental divide of the strategic debate on cyber-defense. I show that although many efforts have been dedicated to understanding the strategic dimensions of cyberspace, a rift prevails between two camps: one predicts the emergence of cyberwarfare while the other characterizes such events as no more than cases of 'cyber-annoyance'. In the second section, I explain that this protracted clash of views comes mainly from the use of two misleading analogies for cyberwarfare: nuclear warfare and strategic bombing. The article then demonstrates in a third section that a middle way to implement a military policy in cyberspace can be found by understanding cyberattacks as a subset of broader military operations. To that end, I employ the tools of campaign analysis to make an appraisal of events such as the cyberattacks against Georgia prior to its August 2008 war against Russia. Finally the article's conclusion explores the implications of my findings for future research.

Cyberwar or cyber-annoyance? The fundamental divide of the strategic debate

In spite of obvious efforts (such as the 2009 60-day *Cyberspace Policy Review*, led by Melissa Hathaway, former Senior Advisor to the US Director of National Intelligence), the Obama administration has not tackled the fundamental dispute over the strategic implications of cyberattacks. Currently in Washington, two opposing views compete with each other: the alarmist voices (and indeed the most vocal ones) who predict the advent of cyberwarfare as a revolutionary form of conflict, and the skeptical voices who acknowledge the "annoying" vulnerabilities of US civilian and military infrastructures but who do not see such attacks as the constituents of a pattern for potential new major conflicts.

This divide has existed since the middle of the 1990s, when the US Department of Defense and military-related think tanks started issuing reports and articles on the strategic implications of cyberspace. Although the cyber realm and information warfare have significantly evolved since then, the terms of the divide have been noticeably constant all along. Starting in the 1990s, an impressive proportion of the strategic studies literature focused on the so-called "Revolution in Military Affairs", of which the optimal exploitation of electronic interfaces was only one of many components. From the futurists Alvin and Heidi Toeffler, and their famous "third wave" characterization of the information revolution,[1] to the iconoclast colonel Richard Szafranski and his fuzzy concept of "neocortical warfare", people inside the Defense Department started to read and write about warfare in the information age.[2] This led to the now famous but still-ambiguous concept known as "information warfare".[3]

The starting point for emerging conceptual debates could be marked in 1993, when John Arquilla and David Ronfeldt, two researchers at the RAND Corporation, published an article titled "Cyberwar is Coming!" in the journal *Comparative Strategy*.[4] Behind this emblematic title, the two

scholars argued that cyberwar - defined as a war centered on information flowing through electronic interfaces - was to provoke a fundamental bottom-up review of military organizations.

Yet straight away, ideas about a war in cyberspace sounded at best farfetched, at worst spurious. After all, was it not a term - cyberspace - taken from a science fiction book?[5] Some researchers saw this conflation of concepts and ideas as an eventual march toward the establishment of a coherent field of studies. For instance, the late Laurent Murawiec, a scholar from the Hudson Institute, observed in 2001 that

> As presently constituted, the field seems to cover a bewildering array of subsets: psychological warfare, deception, cyberwar, critical information protection, computer network attack, computer network exploitation, netwar, and more. The confusion is normal. When people started building automobiles, hundreds, if not thousands of attempts were made which bore the name of "automobile", and other names too. The variety of shapes, methods, materials, solutions proposed to the various problems of a self-propelled vehicle, was equally bewildering. It took time and experience, much competition and failures, to winnow, to rationalize, to weed out. We can only expect the same to hold true in the field of "information warfare" as opened up by the digital revolution of the last quarter century.[6]

But contrary to Murawiec's faith, ten years later, the confusion still remains. Moreover, this decade-long divide has deepened since 2007 as cyber-defense has been put at the forefront of the political-military agenda following the cyberattacks against Estonia in 2007, the use of cyberspace during the military campaign between Russia and Georgia in 2008, and lastly the Stuxnet worm that targeted the Iranian nuclear plant in Natanz in 2010.

Counted among the alarmist voices are recently retired US officials such as Richard Clarke, former Special Advisor to the President on Cybersecurity, and Mike McConnell, former Director for National Intelligence. Mr. Clarke explains in his book, *Cyberwar: The Next Threat to National Security and What to Do About It*, that what states "are capable of doing in a cyber war could devastate a modern nation".[7] In February 2010, Mr. McConnell explicitly titled a much-discussed op-ed from the *Washington Post*, "How to win the cyberwar we're losing".[8]

More specifically, these voices frequently compare the current debate on the scope of cyberwarfare with the age of nuclear strategy in the 1950s. For instance, Mr. McConnell asserts that "the cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects".[9] Following this comparison, they call for a doctrine of cyber-deterrence. Moreover, General Kevin Chilton, the head of US Strategic Command, supports the idea of a combined deterrence based on nuclear weapons, missile defense systems, and cyberwarfare capabilities.

In a US Air Force journal, Chilton wrote that "the deterrence impacts of such uncertainty over the potential impacts of a cyberspace attack would be a function of the nature of the attacker's goals and objectives. A competitor's concerns about unintended consequences could enhance the effects of our deterrence activities if it wishes to control escalation or fears blowback from its cyberspace operations".[10] This fairly resembles the Cold War's MAD (Mutually Assured Destruction) doctrine. Originally emerging at the end of the Kennedy administration, MAD was a doctrine that assured that a full-scale use of nuclear weapons by two opposing sides would effectively result in the destruction of both the attacker and the defender.[11] Can such an argument be replicated into cyberspace? So far, it is hardly conceivable.

As a matter of fact, one year prior to Chilton's article, a suggestion from a US military officer was already raising similar questions. In May 2008, Colonel Charles Williamson from the US Air Force

wrote a widely criticized article in the *Armed Forces Journal* on the potential build-up of military botnets that could be used for offensive purposes.[12] For Williamson,

> America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack.[13]

In other words, Williamson was not only acknowledging an on-going arms race in cyberspace, he was advocating it. But Williamson was only adding another argument to the idea that cyberspace in itself is a new and separate domain of warfare. This idea had grown in earnest several months before his article, when Estonia experienced cyberattacks against its governmental servers. Following the attacks, the US Secretary of the Air Force, Michael Wynne, stated that "Russia, our Cold War nemesis, seems to have been the first to engage in cyber warfare".[14] Jaak Aaviksoo, Estonian Minister of Defense, went further, evoking "the first unnoticed third world war".[15]

But even while these voices are urging for a new posture toward cyberwarfare, skeptical voices—among them Howard Schmidt, the current Cybersecurity Coordinator for the Obama Administration—are vigorously opposing their conclusions. Although such thinkers recognize the need for improving information system security, they understand the concept of cyberwarfare as deeply flawed. For instance, Schmidt stated during an interview at the RSA Security Conference in San Francisco in March 2010: "There is no cyberwar [...] I think that is a terrible metaphor and I think that is a terrible concept".[16]

All in all, both postures (the alarmist and the skeptical) fuel the debate in Washington, both in the government and in think tanks. This rift has two consequences: first, the US military still remains uncertain precisely what cyberwarfare, cyberconflict or, indeed, any other term given to describe the political use of attacks in the cyberspace actually stands for. Second, this tension logically affects the credibility of the national security architecture, leading to official disagreements on the threat level (e.g. Howard Schmidt stating publicly that 'there is no cyberwar'[17]) or even interservice rivalries (the Air Force having claimed since 2005 to be the one to 'fly and fight in cyberspace'[18]). But the rift between these two antagonistic views can and should be overcome. This is the aim of the next two sections, starting with how the confusion is produced by two analogies—nuclear warfare and strategic bombing—that too often frame the debate on cyber military policies.

The problems of current analogies for cyberwarfare

Balancing the equation between the alarmists and the skeptics of cyber-threats requires a critical examination of the terms of the debate, and more specifically of the frequently used analogies. The study of new phenomena in international affairs is often dependent on analogical reasoning. Analogies provide guideposts on the assumption that new issues can be understood within the framework of older, more familiar ones. Regarding cyberspace, two analogies have been extensively used, both explicitly and implicitly: cyberwarfare as nuclear warfare, and cyberwarfare as strategic bombing. Each is misleading.

The analogy with nuclear warfare is often used to emphasize the low level of existing knowledge on the strategic implications of cyberattacks. Within that logic, the same could be said of the early nuclear literature published in the 1950s and 1960s. At that time, no one denied the potentialities of

nuclear weapons, as they were dramatically demonstrated at Hiroshima and Nagasaki. But equally, no one could accurately appraise how nuclear forces and their diffusion would alter the balance of power in the context of the Cold War. It took years and some risky and bold analysis from Bernard Brodie, Herman Kahn, and Albert Wohlstetter to build a more coherent understanding of nuclear strategy.[19] People needed to "think the unthinkable", to cycle through numerous ideas and concepts in order to finally build a coherent intellectual framework for nuclear policy analysis.[20]

The comparison with cyberwarfare, however, cannot be stretched further. While nuclear weapons remain the single most lethal asset available to armed forces, in terms of military applications, cyberattacks do not have any direct lethal effect. In terms of force employment, the cyberattacks perpetrated in recent years have tended to be used in support of combined operations (the Russia-Georgia war of 2008) with low-intensity effects, or to achieve a modest political outcome (the intimidation of Estonia in 2007). By contrast, nuclear warfare—at least since the widespread acceptance of the MAD doctrine—has been understood to carry the real risk of escalation to a Clausewitzian absolute conflict that shifts the strategic calculus of conventional warfare. Deterrence in the nuclear field is relevant because of its absolute character. Cyberattacks can disrupt the command and control systems of an enemy, but they do not annihilate his population.

Furthermore, computer scientists underline that technical limitations prevent the victim of a cyberattack from identifying their attacker in cyberspace, which results in an inability to deter a potentially anonymous aggressor. Indeed, with the current state of technology, cyberattacks deny the technological possibility to trace their origins. The use of botnets implies the hijacking of computers that can be located in other countries, or even on other continents. Therefore, authorities do not have any certainty with which to attribute an attack to a terrorist organization or to a state. For instance, cyberattacks on Estonia in spring 2007 were partly originating from computers physically located in California. Therefore, for all these reasons, cyberattacks can barely be compared to nuclear strikes.

The second analogy refers to strategic bombing, a theory of coercion based on the exploitation of massive air attacks that emerged at the end of the First World War and that has, for much of the period since, constituted a dogma of the US Air Force in its claims for the independent effectiveness of airpower. As Caroline Ziemke wryly observed: "Strategic bombing is not mere doctrine to the USAF; it is its lifeblood and provides its entire *raison d'être*. Strategic bombing is as central to the identity of the Air Force as the New Testament is to the Catholic Church".[21] In other words, the fact that strategic bombing is USAF's *raison d'être* demonstrates how the US armed forces can acquire technological obsessions as a product of their strategic culture, even when the empirical evidence does not systematically support their position.

The presumed similarity between cyberattacks and strategic bombing has already led several pundits to argue for an explicit cyberpower doctrine, recalling directly the long and intractable debate over the independent effects of airpower.[22] Institutionally, this analogy can be explained as a product of the US Air Force's sunk investment in cyberspace expertise. But more particularly, this analogy emphasizes the persistently technology-centered nature of US strategic culture.[23]

In other words, the analogy is based on the idea that technological capabilities (whether air strikes or cyberattacks) can compel the enemy to do our will without ever launching a massive and costly ground offensive.[24] But in spite of certain thinkers' enduring faith, there is little evidence that strategic bombing has ever decisively determined victory in war.[25] Regarding cyberattacks, there is even less proof that they have been decisive in any military context.

The best example of this misleading analogy is the contemporary debate surrounding the Stuxnet attack against the Iranian uranium-enrichment plant in Natanz. After rumors spreading in the summer of 2010, the authorities in Tehran acknowledged in November that the control systems of its nuclear facilities had been targeted by a cyberattack that caused significant physical damage. There is clear evidence from the reports issued by the International Atomic Energy Agency that the cyberattacks targeting the centrifuges delayed for about a week Iran's nuclear program. Nevertheless, Stuxnet did not decisively stop Tehran's ambition, it only hindered the pace of its fulfilment.[26] Thus, the exaggerated statements on Stuxnet and the advent of cyberwar *per se* come from this same belief about strategic bombing and its decisiveness.

Consequently the analogy is not applicable, not strictly because cyberattacks lack the lethality of air strikes (they actually could resemble air strikes in terms of disruptive effects), but because the analogy is biased by the fundamental assumption that strategic bombing can be decisive and so cyberattacks could as well.

Although the errors vary for the respective different comparisons with nuclear warfare or strategic bombing, one common conclusion can be drawn: as of today, cyberattacks do not amount to a distinct field of warfare with its own rules and processes. Both analogies should therefore be avoided if we are to get the conceptual framework for the analysis of cyberattacks right. Therefore, we need to strictly understand the history of the phenomenon within the context of military operations.

A middle way for a military posture in cyberspace

The political science literature dedicated to campaign analysis can provide precious insights on how to articulate a robust strategic analysis of cyberattacks that avoids both the fads of "cyberwarmongers" and the reductionist arguments of "cyberskepticals". Campaign analysis looks at the operational level of military activity by combining an appraisal of the objectives, the military balance (quantity, quality, joint capabilities), the terrain, the duration of the campaign and its evolution (breakthrough, maneuver).[27] Going beyond a simple compilation of military resources and technologies, this methodology allows us to get a better grasp of how these assets are used *during* the campaign, what Stephen Biddle calls the "force employment" factor.[28]

So far, campaign analysis has rarely looked at cyberattacks. The most obvious reason is the lack of sufficient available data (due to the classification issue) that would be needed. Nevertheless, based on the first lessons learned from the cyberattacks released to the public (mostly about the Estonian and the Georgian cases), cyberwarfare cannot be described as an independent field of warfare. There cannot be war in cyberspace like there are instances of wars in the air, on the seas, or on land. Cyberattacks can only be conceived as a component by-product of a larger military campaign. In other words, a cyberconflict has to be defined as a proxy conflict aimed at attaining an intermediate goal for an attacker, thereby functioning as a subsidiary addition to conventional kinetic military operations. Cyberattacks are means of denial, not of punishment: they can block an enemy's ability to use its information systems as part of their war effort, but they are rarely designed to achieve political outcomes in their own right by inflicting an unbearable cost on the defender.[29]

On that matter, the lessons learned from the cybercampaign against Georgia during the war in Russia in August 2008 are instructive. Georgia experienced early cyberattacks in late July, including an attack on the presidential website on July 19. Due to a distributed denial of service attack, the

website remained unavailable for twenty-four hours.[30] After a two week pause, cyberattacks targeting Georgian government and media websites started by late August 7 following President Mikheil Saakashvili's decision to attack South Ossetian separatist forces that night. But the wave of attacks substantially increased on August 8, the day the Russian armed forces entered Georgia, when cyberwarriors began to block and deny access to Georgian govermental websites, and moved on to expand the list of targets to include financial institutions.[31]

Experts from the US Cyber Consequences Unit (US CCCU) surmised that the attackers were civilians recruited through electronic social networks. However, more significantly, the authors of the report concluded that there was a clear convergence between the Russian armed forces' campaign and the hackers' actions: "The organizers of the cyber attacks had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out".[32] Consequently, this illustrative case of cyberwarfare clearly demonstrates the integration of such practices into a larger military campaign. By themselves, cyberattacks function as proxy components of a strategic offensive. Indeed, one could argue that the use of cyberattacks during the conflict between Russia and Georgia pointed away from the use of autonomous cyberwarfare in itself, and instead illustrated that there are combined operations that can exploit cyberattacks in the same way that theater air campaigns have been performed for decades.

Interestingly, this also happens to be the way that Chinese strategists conceive the exploitation of cyberspace. In spite of misleading speculations regarding Chinese capabilities (mainly a consequence of the alarm generated by the best-selling book *Unrestricted Warfare*, written in 1999 by PLA colonels Qiao Liang and Wang Xiangsui), the People's Liberation Army (PLA) does not conceive cyberspace as an autonomous military domain.[33] Rather, the Chinese military has explicitly adopted a posture including the concept of "integrated network electronic warfare", which aims at controlling the flow of information in the adversary's system and at maintaining the PLA's information superiority on a traditional, physical battlefield. Moreover, the seminal Chinese documents, *The Science of Military Strategy* and *The Science of Campaigns*, both underline the decisive role of information superiority in air and sea warfare.[34] Such strategic thought clearly integrates cyberattacks into classic military campaigns. In short, even thinkers in the United States' principal future great power rival only see cyber as a subcomponent of modern conventional conflicts.

In spite of all the political exaggerations regarding cyberwarfare, modern cases (Estonia in 2007, Georgia in 2008, the revelations over a so-called 'GhostNet' operating against Tibetan authorities) display evidence that there are no truly independent or even autonomous cyberwars *per se*.[35] In all of these instances, cyberattacks were a component by-product of a larger campaign (political intimidation in the Estonian and Tibetan cases, military intervention in the Georgian case).

As a result, our assessment renders debate on the future of deterrence in cyberspace irrelevant. Of course, this does not mean that hackers cannot inflict significant damage that could severely disrupt the vital infrastructure of a country but so too, still, could bombers and tanks. Even worst-case scenarios involving cyberattacks do not suggest that the United States or other major powers could be severely coerced, let alone existentially threatened, by such cyberattacks alone.

The belief that disruptions in cyberspace could defeat a country is flawed—and dangerous. The idea that cyberwarriors could become the principal combatants of a future war without physical implications remains science fiction *à la* William Gibson. It might be the role of strategic futurists to explore such narratives, but policy-makers that need to base analysis on present-day objective facts have to acknowledge this evidence: taking into account recent international events and known

technological trends, cyberattacks cannot be compared to nuclear warfare. The actual analogy that should be explored, if such analogical reasoning is cognitively necessary to conceptualize and understand the emergence of cyberattacks, is electronic warfare. It may be less strategic and more technical, but it is also more relevant.

◆ ◆ ◆

Policy-makers and military planners should neither overestimate the strategic scope nor underestimate the operational effectiveness of cyberattacks. The protracted battle over their significance has not only intellectual implications but policy ones as well. The inability of the Obama administration to bridge this decade-long gap between these two distinct views of cyber-defense extends the institutional dysfunction into the current system. Alarmists and skeptics are dispersed in all levels of the chain of command (in the White House, the Department of Homeland Security, the Department of Defense, the National Security Agency or the Department of State) without anyone prevailing. As a result, final decisions are still taken as a product of bureaucratic tactics, rather than on the back of cautious strategic threat-assessment.[36]

Therefore, getting the strategic appraisal right should be the priority when designing the relevant military posture. As I explained in this article, there is a middle ground between dismissing the military significance of cyberattacks and overestimating their reach. Cyberattacks certainly represent a cost-effective tool to support classic land, sea and air campaigns, and consequently their military added-value should be assessed in the context of joint operations. But they do not represent a new and revolutionary class of military operation in their own right.

In the coming years, the challenge will be precisely to measure this added-value, whether in offense or in defense, and at both the national armed forces level and the joint international level. Policy makers and strategic analysts should then increase their efforts on the exploitation of two techniques helpful to adapt a military posture in cyberspace:

- First, thorough campaign analysis of recent cyberattacks can provide precious assessments of the "force employment" factor in cyberspace and its effectiveness on the battlefield. It will permit the US military to shift its focus from cybertechnology as the decisive assets to a posture based on an optimal exploitation of these weapons in the context of combined operations to achieve strategic objectives;

- Second, scenario-based exercises should look at how US armed forces can operate in a *degraded* cyber environment.[37] Exploring specific contingencies where cyberattacks would disrupt the conduct of an operation, these exercises should not only involve national servicemen but also the militaries from NATO members as well as from traditional allies (Japan, South Korea). This will provide new evidence and ideas on how to integrate these engagements as an additional contributory element to a broader military campaign.[38]

This adaptation process could well represent the key to both defensive resilience and offensive edge when confronting future cyber-threats.

About the Author

Jean-Loup Samaan is a policy advisor at the French Ministry of Defense (Directorate for Strategic Affairs) and an adjunct lecturer in international security at the French Institute for Political Studies, Sciences Po. A former visiting scholar at the RAND Corporation and Duke University, he holds a PhD in Political Science from the University of Paris. The views expressed in this article are his only, and do not necessarily reflect those of the French government.

Notes

1 Alvin Toffler, *The Third Wave*, (New York, NY: Bantam Books, 1980).

2 Richard Szafranski, 'Neocortical Warfare? The acme of skill' in John Arquilla, David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica CA: RAND Corporation, 1997), pp.395-416.

3 Although the term was initially conceived by Thomas Rona in a corporate document from the Boeing Company, in 1973. See Thomas P. Rona, *Weapon Systems and Information War*, (Seattle, WA: Boeing Aerospace Co., 1976).

4 John Arquilla, David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy*, (Vol.12, No.2, Spring 1993), pp.141-165.

5 William Gibson, *Neuromancer*, (New York: NY, Ace Hardcover, 1994).

6 Laurent Murawiec, *Aristotle in Cyberspace: toward a theory of information warfare*, (Santa Monica, CA: RAND Corporation, 2001), p.26.

7 Richard Clarke, Robert Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, (New York: NY, HarperCollins, 2010), p. 31.

8 Mike McConnell, 'How to win the cyberwar we're losing'*, Washington Post,* 28 February 2010.

9 *Ibid.*

10 Kevin Chilton, Greg Weaver, 'Waging Deterrence in the Twenty-First Century', *Strategic Studies Quarterly*, (Vol.1, No.3, Spring 2009), p.40.

11 Among others, Alan Parrington, 'Mutually Assured Destruction Revisited: Strategic Doctrine in Question', *Airpower Journal*, winter 1997; Henry Sokolski, *Getting Mad: Nuclear Mutual Assured Destruction, its Origins and Practice*, Strategic Studies Institute, 2004.

12 Charles Williamson, 'Carpet bombing in Cyberspace', *Armed Forces Journal*, May 2008.

13 *Ibid.*

14 Rebecca Grant, *Victory in Cyberspace*, Air Force Association, 2007.

15 Estonian Ministry of Defense news release, 'Internet : XXI Century Battlefield', 16 June 2007.

16 Ryan Singel, 'White House Cyber Czar: There Is No Cyberwar', *Wired.com*, 4 March 2010. Accessed 6 0ctober 2010. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

17 Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar'", *Wired*, 4 March 2010.

18 See Sebastian Convertino, Lou Anne DeMattei, Tammy Knierim, *Flying and Fighting in Cyberspace*, (Alabama, Air War

College, Maxwell Paper No.40, 2007).

[19] Fred Kaplan, *The Wizards of Armageddon*, (New York, NY: Simon and Schuster, 1983).

[20] Herman Kahn, *Thinking about the Unthinkable*, (New York, NY: Horizon Press, 1962).

[21] Caroline Ziemke, 'Foreword' in TILFORD Earl, *Setup: What the Air Force Did in Vietnam and Why*, (Maxwell, Air University Press, 1991), p. ix.

[22] See Rebecca Grant, *Victory in Cyberspace*; Frank Kramer, Stuart Starr, Larry Wentz, *Cyberpower and National Security*, (Washington D.C.: NDU Press, 2009).

[23] On this debate, see Russell Weigley, *The American Way of War: A History of United States Military Strategy and Policy*, (Indiana: IN, Indiana University Press, 1977); Antulio Echevarria, *Toward An American Way of War*, (Washington, Strategic Studies Institute Monograph, 2004); Colin Gray, *Irregular Ennemies and the Essence of Strategy: Can the American Way of War Adapt ?*, (Washington, Strategic Studies Institute Monograph, 2006); Arthur Cebrowksi, Thomas Barnett, 'The American Way of War', *Proceedings*, January 2003.

[24] On this belief, see the literature following the Desert Storm campaign: Christopher Bowie, David Ochmanek, Fred Frostic, Kevin Lewis, John Lund, Philip Propper, *The New Calculus: Analyzing Airpower's changing role in joint theater campaigns*, Santa Monica, RAND Corporation, 1993; Eliot Cohen, 'The Mystique of U.S. Air Power', *Foreign Affairs*, (Vol.73, No.1, 1994);

[25] See Robert Pape, *Bombing to Win: Air Power and Coercion in War*, (Ithaca: NY, Cornell University Press), 1996 and one of its critics, Barry Watts, 'Ignoring reality: Problems of theory and evidence in security studies', *Security Studies*, (Vol 7, No.2., Winter 1997-1998), pp. 115-171

[26] On the assessment of the Stuxnet attacks, see International Institute for Strategic Studies, "Stuxnet: targeting Iran's nuclear programme", Strategic Comments, February 2011; James Farwell, Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, (Vol.53, No. 1, February-March 2011), pp.23-40; Isaac Porche, "Stuxnet is the world's problem", *Bulletin of the Atomic Scientists*, 9 December 2010; Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Symantec, February 2011.

[27] Among others, see John J. Mearsheimer, "Why the Soviets Can't Win Quickly in Central Europe," *International Security*, (Vol. 7, No. 1, Summer 1982), pp.139-175; Barry R. Posen, *Inadvertent Escalation*, (Ithaca, N.Y.: Cornell University Press), pp. 68-128.

[28] See Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*, (Princetion : NJ, Princeton University Press, 2004).

[29] See for instance the distinction made by Martin Libicki between strategic cyberattack and operational cyberattack while exploring the scenarios of a China-US contingency in Martin Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy*, (Santa Monica, CA: RAND Corporation), January 2011.

[30] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defence Centre of Excellence, Estonia, 2008, p.36.

[31] Ronald Asmus, *A Little War That Shook The World*, (New York, N.Y.: Palgrave, 2010), p.166; John Bumgarner, Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia In August of 2008*, US-CCU Special Report, US Department of Defense, August 2009, p.5.

[32] Bumgarner, Borg, *Overview by the US-CCU*, p.3.

[33] Qiao Liang, Wang Xiangsui, *Unrestricted Warfare*, (Panama, Pan American Publishing Company, 2002).

[34] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*,

Report from Northrop Grumman to the US-China Economic and Security Review Commission, October 2009, pp.6-7; Gurmeet Kanwal, 'China's Emerging Cyber War Doctrine', *Journal of Defence Studies*, (Vol.3, No.3, July 2009), pp. 14-22.

[35] Information Warfare Monitor, *Tracking Ghostnet : Investigating a Cyberespionnage Network*, March 2009.

[36] For a cautious analysis of the US reforms in cyberdefense, see CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, (Washington: DC, Center for Strategic and International Studies), February 2011.

[37] Noticeably, the new *US National Military Strategy* released in February 2011 acknowledges the need to better apprehend the conduct of operations in "degraded environments".

[38] An illustration of such valuable scenarios is provided by Martin Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy: Two Scenarios*, (Santa Monica: CA, RAND Corporation, 2011).

The Vulnerability of Nuclear Facilities to Cyber Attack

Brent Kesler

Introduction

In June 2010, U.S. Senators Susan Collins, Joseph Lieberman, and Tom Carper introduced the Protecting Cyberspace as a National Asset Act. One of its many aims is to protect critical infrastructures in the United States from cyber attack. In January 2011, Brandon Milhorn, staff director of the Senate Homeland Security and Governmental Affairs Committee, defended the bill, saying that it would prevent a hacker from opening the floodgates of the Hoover Dam. Peter Soeth, a spokesman for the US Bureau of Reclamation, the agency which manages the Hoover Dam, objected to that example, arguing that "These types of facilities are protected by multiple layers of security, including physical separation from the internet, that are in place because of multiple security mandates and good business practices."[1]

This dispute over the Hoover Dam demonstrates the classic pattern of debate over critical infrastructures and their vulnerability to cyber attacks. Most of the process control systems designed to manage critical infrastructures, such as electric grids, oil pipelines, and water utilities, use specialized hardware and proprietary protocols. However, since the 1990s, the managers of these infrastructures have been integrating their control systems with computer networks built from commercial off-the-shelf operating systems, such as Windows and Unix.[2] This has simplified the task of managing facilities remotely, but it has also made process control systems vulnerable to attack over the internet. Alarmists point to these connections as vulnerabilities that pose almost epic threats; skeptics immediately dismiss such fears, claiming that the necessary measures to prevent a catastrophic cyber attack have already been implemented. History suggests the truth lies somewhere in between.

As a relatively young field, national cyber security policy has been open to speculation about potential threats. However, in 2011, network operators have accumulated enough experience and data from real world attacks to draw a more realistic picture of the threats facing critical infrastructures. This paper will examine the history of cyber security incidents at nuclear facilities to assess the extent to which recorded vulnerabilities pose an "epic" threat. Specifically, it will examine three cyber incidents that occurred at U.S. nuclear facilities between 2003 and 2008. It will then turn to details of the 2010 Stuxnet attack against the Iranian nuclear program to outline similarities with the three U.S. incidents. The lessons from these four incidents suggest that situational awareness and other security measures are too weak in their current state to guarantee that a catastrophic attack will never happen. However, it will also argue that launching a catastrophic attack is not simple and requires a sophisticated adversary. The article will then turn to gaps in nuclear regulation that policy makers should consider when formulating cyber security policies, not only for nuclear facilities, but for other critical infrastructures.

---

1 David Kravets, "No, Hackers Can't Open Hoover Dam Floodgates" *Threat Level,* (*Wired* blog), February 3, 2011. http://www.wired.com/threatlevel/2011/02/hoover/

2 Martin Stoddard et al, *Process Control System Security Metrics – State of Practice*, Institute for Information Infrastructure Protection, August 2005.

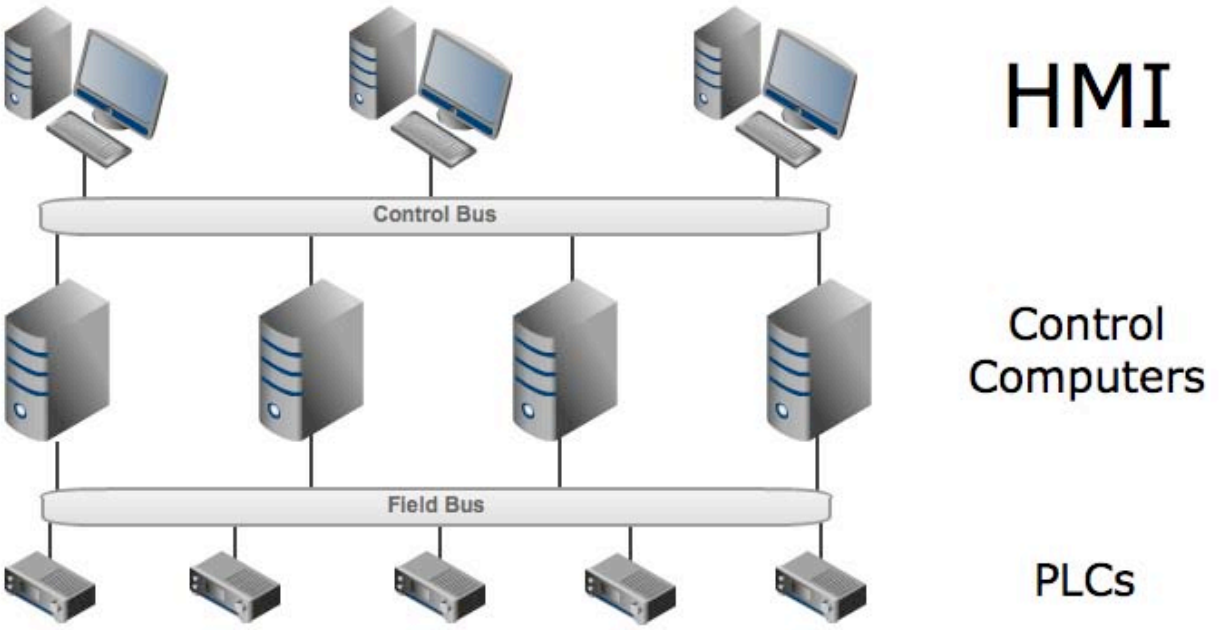


Figure 1: Highly simplified representation of a process control network

Process control systems

Historically, critical infrastructures have used two kinds of control systems: supervisory control and data acquisition (SCADA) systems that quickly gather remote field data, and distributed control systems (DCS) that manage automated manufacturing processes. Over time, these systems began to share many of the same technologies and features, making them less distinct from each other. However, given their separate histories, much of their distinct terminology remains. Other terms, such as integrated control systems (ICS) or instrumentation and control (I&C) are also used, depending on the traditional practice of the facilities using these systems. This paper will collectively refer to these technologies as process control systems (PCS). [3]

Process control systems come in any number of complex architectures, but a general pattern holds for most facilities. The *control network* is the collection of computer systems which directly monitor and control plant operations. At the top are the *human-machine interfaces* (HMI) that display data from plant equipment and allow technicians to adjust their operations. These are often Windows or Unix based computers. HMI communicate over a *control bus* with other computers that monitor and control operations using software that is less user-friendly. These computers communicate over a *field bus* with *programmable logic controllers* (PLC), hardware that directly adjusts the various motors, sensors, actuators, and other physical components at the heart of a plant's operations.[4] This is a highly simplified description of a control network; structure and terminology will vary.

Power plants also have office networks for business purposes. The office networks often collect data from control networks and have connections with a wider corporate network over the internet.

3 Stoddard et al, *PCS Security Metrics.*

4 K. Korash et al. *Emerging Technologies in Instrumentation and Controls: An Update.* (Oak Ridge: Oak Ridge National Laboratory, 2006), 25-28.

Connecting control networks with business offices and the larger corporate network makes it easier for managers to match plant operations with business goals and improve efficiency. However, it also opens a path that malicious hackers on the wider internet could follow to the plant's process control systems.

Vulnerability of process control systems

Operators of process control systems used to believe they were invulnerable to cyber attack for two main reasons. The first reason is the assumption that PCS are isolated from the internet; the second is that PCS generally use proprietary protocols and specialized hardware not compatible with ordinary computers and common network protocols like Ethernet and TCP/IP. These assumptions have led some PCS operators to see the threat of a cyber attack as alarmist. For example, a 2002 article published in *CIO Magazine* outlines the numerous security precautions taken by the Massachusetts Water Resource Authority (MWRA) and concludes that a cyber attack against its PCS would have no effect:

> [M]ost public utilities rely on a highly customized Scada system. No two are the same, so hacking them requires specific knowledge -- in this case, knowledge of the MWRA's design and access to that customized software. ... Scada is not networked, except in two places. [5]

He added:

> [PLCs] follow the lowest level, most basic instructions (such as turn on and turn off), and report them to Scada ... If something is wrong, the PLC says, "Help me" in the form of an alarm. The alarm sounds at the water site and at the Scada operations centers. The alarm also flashes on the computers, and it can't be shut off until a formal acknowledgement of the alarm is made and physically logged by a human being[6].

However, many operators have been moving towards open protocols and off-the-shelf hardware to manage their process control systems, even connecting them to the internet—sometimes inadvertently.[7] These trends have made PCS vulnerable to hackers, often with dangerous results. This fact had been demonstrated even before the MWRA article and has been repeatedly confirmed by penetration testers hired to assess cyber security at critical infrastructures. At the 2006 Black Hat Conference, presenters from IBM Internet Security Systems' X-Force team outlined a penetration test at an unnamed power plant. While meeting with plant management in a conference room, the testing team found a unprotected wireless access point, used it to access the plant's business network, and from there accessed the plant's control network using a ten-year old exploit. In X-Force's experience, only knowledge of common internet protocols was necessary to interfere with PCS systems, but any hacker who wanted to take the extra step to learn about PCS protocols could

5 Scott Berinato. "Debunking the Threat to Water Utilities", CIO Magazine (March 15, 2002). http://www.cio.com/article/30935/Debunking_the_Threat_to_Water_Utilities

6 Ibid.

7 A common cause of an inadvertent connection is a "rogue access point". Employees sometimes set up a wireless network in their office without telling systems administrators. If the access point is not well protected, a hacker can use it to bypass the firewalls and intrusion detection systems that administrators have set up to protect office computers from the wider internet.

find technical specifications online.[8]

Past PCS attacks have even caused physical damage to critical infrastructures. For example, in 2000 a former contractor hacked into the Maroochy Water District's PCS system in Queensland, Australia, and released 80,000 liters of raw sewage into parks, rivers, and even the Hyatt Regency Hotel; the smell drove away local residents, river water turned black, and marine life died as a result.[9] In March 2007, Idaho National Laboratory conducted a test of the so-called "Aurora vulnerability". This vulnerability would allow an attacker at a remote high voltage circuit breaker to physically destroy a generator by quickly opening and closing the breaker. Details of this vulnerability have been designated "For Official Use Only" by the Department of Homeland Security.[10]

Cyber attacks against PCS, whether intentional or unintentional, are likely underreported. No regulation exists requiring power plants to report problems with or attacks against their control systems. In the case of the Aurora vulnerability, ES-ISAC (Electric Sector Information Sharing and Analysis Center) and the Nuclear Energy Institute issued advisories that required no action.[11] In April 2009, the North American Electric Reliability Corporation (NERC) issued a letter stating that many power companies were choosing not to identify critical assets in order to avoid complying with cyber security standards, leaving them exposed to such vulnerabilities as Aurora.[12] NERC explains this behavior as a misconception of cyber threats; most operators do not see their own systems as critical to the Bulk Electric System, so they fail to realize that a cyber attack could affect multiple systems at once, and through them the power grid as a whole. In another case, an unnamed power plant suffered a targeted attack and lost process control systems for two weeks. However, since the attack did not disrupt power generation, the attack was not reported to government agencies.[13]

Process control systems at nuclear power plants

The United States has 104 nuclear power plants generating 98,000 megawatts of electricity, roughly 20% of the electricity generated within the US. These plants generally have process control systems, often designed by the same companies that provide these systems to non-nuclear power plants.[14] However, the operators of non-nuclear plants usually have better hardware and cyber security experience than their colleagues at nuclear facilities. Since installation and upgrades of PCS are

8 David Maynor and Robert Graham. "SCADA Security and Terrorism: We're not crying wolf", (paper presented at the Black Hat conference, Las Vegas, Nevada, July 29-August 3, 2006). http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

9 Marshall Abrams and Joe Weiss. "Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia" National Institute of Standards and Technology, Computer Security Resource Center (August 2008). http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

10 Joe Weiss. "One reason why we need regulation", *ControlGlobal.com Unfettered Blog* (December 18, 2008). http://community.controlglobal.com/content/one-reason-why-we-need-regulation

11 Ibid.

12 Michael Assante. "Critical Cyber Asset Identification" (Letter to Industry Stakeholders from the North American Electric Reliability Corporation, April 7, 2009). http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf

13 Joe Weiss. "Control system cyber events, 60 Minutes, disclosure, and FUD", *ControlGlobal.com Unfettered Blog* (November 13, 2009). http://community.controlglobal.com/content/control-system-cyber-events-60-minutes-disclosure-and-fud

14 Ken Barnes, Briam Johnson, and Reva Nickelson. *Review of Supervisory Control and Data Acquisition (SCADA) Systems*, Idaho National Engineering and Environmental Laboratory, January 2004, page 9.

costly and time-consuming, most non-nuclear PCS operate for eight to fifteen years, the expected lifespan of the hardware used. However, nuclear plants face even higher costs and more stringent safety requirements for their PCS, so they often choose to continue using their original control systems rather than upgrade. A nuclear PCS can be in service for twenty to thirty years, well past the life expectancy of the hardware. Many plants are still using systems based on analog electronics rather than digital.[15] This is confirmed by the experience of nuclear engineer Joe Weiss, now a managing partner of Applied Control Solutions, a consultancy specializing in control system cyber security. Mr. Weiss worked for five years managing a nuclear instrumentation program for the Electric Power Research Institute (EPRI). However, nuclear plants prefer to use tested technologies so Mr. Weiss did not get to do "bleeding edge" research until he managed EPRI's research program for fossil fuel plant instrumentation. This meant that nuclear plants had often adopted modern information technology for their process control systems, but had less experience implementing cyber security on those systems than their colleagues at other electric power plants. This experience gap often led nuclear operators to assume they were less exposed to cyber threats than non-nuclear power plants.[16]

In the past five years, US government-funded research into the cyber security of process control systems has focused mainly on oil and gas utilities and the electric grid. While nuclear power plants face many of the same issues in protecting their infrastructure, the key difference is the nuclear reactor. Non-nuclear generators can be completely shutdown, but nuclear reactors run for one to two years once the fuel is installed. Even when the reactor is "shutdown", the fuel still produces decay heat and must be cooled, or the reactor core may melt. The partial meltdown of Three-Mile Island Unit 2 occurred during a reactor shutdown due to operator errors and equipment malfunctions.[17] If such errors and malfunctions can be replicated by a cyber attack, then a reactor meltdown is possible. To determine the danger of this threat, it is necessary to examine cyber incidents that have occurred at nuclear power plants.

Davis-Besse worm infection

On January 25, 2003, at 12:30 AM Eastern Standard Time, the Slammer worm began exploiting a vulnerability in Microsoft SQL Server. Within ten minutes, it had infected 75,000 servers worldwide—90% of vulnerable hosts. The design of Slammer was simple; it did not write itself to the hard drive, delete files, or obtain system control for its author. Instead, it settled in system memory and searched for other hosts to infect. Removing the worm was as simple as rebooting the server after closing network port 1434, Slammer's point of entry. Installing a patch Microsoft had released six months earlier would eliminate the vulnerability Slammer exploited and prevent another infection.

Although Slammer carried no malicious payload, it still caused considerable disruption. It searched for new hosts by scanning random IP addresses. This generated a huge volume of spurious traffic, consuming bandwidth and clogging networks. Slammer's random IP scans disabled data-entry terminals at a 911 call center in Bellevue, Washington (population 680,000), shutdown 13,000 Bank of America ATMs, and forced Continental Airlines to cancel several flights when their online

15 Ibid, page 23.

16 Joe Weiss. "Nuclear plant cyber security has a ways to go", *ControlGlobal.com Unfettered Blog*, March 25, 2008. http://community.controlglobal.com/content/nuclear-plant-cyber-security-has-ways-go

17 Ronald L. Krutz. *Securing SCADA Systems.* (Indianapolis: Wiley Publishing, 2006), 29.

ticketing system and kiosks could not process orders.[18] South Korea suffered a nationwide internet outage lasting half a day.[19]

The Slammer worm also infected computer systems at the Davis-Besse nuclear power plant near Oak Harbor, Ohio. The worm traveled from a consultant's network, to the corporate network of First Energy Nuclear, the licensee for Davis-Besse, then to the process control network for the plant. The traffic generated by the worm clogged the corporate and control networks. For four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System (SPDS), which shows sensitive data about the reactor core collected from coolant systems, temperature sensors, and radiation detectors—these components would be the first to indicate meltdown conditions. Power plants are required to notify the NRC if an SPDS outage lasts longer than eight hours.

The reactor at Davis-Besse had been offline for nearly a year before its Slammer infection due to the discovery of a hole in the reactor head.[20] Although Slammer's scanning traffic did block sensors from providing digital readouts to control systems, it did not affect analog readouts on the equipment itself; plant technicians could still get reliable data from sensors by physically walking up to them and looking at them, though this process is slower than retrieving data over a network.

Davis-Besse had a firewall protecting its corporate network from the wider internet, and its configuration would have prevented a Slammer infection. However, a consultant had created a connection behind the firewall to the consultancy's office network. This allowed Slammer to bypass the firewall and infect First Energy's corporate network. From there, it faced no obstacle on its way to the plant control network. In response, First Energy set up a firewall between the corporate network and the plant control network.

The Davis-Besse incident highlighted the fact that most nuclear power plants, by retrofitting their SCADA systems for remote monitoring from their corporate network, had unknowingly connected their control networks to the internet. At the time, the NRC did not permit remote operation of plant functions.[21] That policy would change by 2008.

Browns Ferry shutdown

The August 19, 2006, shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama, demonstrates that not just computers, but even critical reactor components, could be disrupted and disabled by a cyber attack. Unit 3 was manually shutdown after the failure of both reactor recirculation pumps and the condensate demineralizer controller.[22] Without the recirculation pumps, the power plant could not cool the reactor, making a shutdown necessary to avoid melting the reactor core.

---

18 Robert O. Harrow, Jr. "Internet Worm Unearths New Holes", *SecurityFocus* (January 29, 2003), http://www.securityfocus.com/news/2186

19 Stacy Cowley and Martyn Williams. "Slammer Worm Slaps Net Down, But Not Out" *PCWorld* (January 25, 2003), http://www.pcworld.com/article/108988/slammer_worm_slaps_net_down_but_not_out.html

20 Kevin Poulsen. "Slammer worm crashed Ohio nuke plant network", *SecurityFocus* (August 19, 2003), http://www.securityfocus.com/news/6767

21 Ibid.

22 US Nuclear Regulatory Commission. "Effects of Ethernet-based, non-safety related controls on the safe and continued operation of nuclear power stations" *NRC Information Notice* (April 17, 2007).

The condensate demineralizer is a kind of programmable logic controller (PLC); the recirculation pumps depend on variable frequency drives (VFD) to modulate motor speed. Both kinds of devices have embedded microprocessors that can communicate data over Ethernet, a popular standard for local access networks (LAN). However, both devices are prone to failure in high traffic environments. A device using Ethernet broadcasts data packets to every other device connected to the network. Receiving devices must examine each packet to determine which ones are addressed to them and to ignore those that are not. It appears the Browns Ferry control network produced more traffic than the PLC and VFD controllers could handle; it is also possible that the PLC malfunctioned and flooded the Ethernet with spurious traffic, disabling the VFD controllers; tests conducted after the incident were inconclusive.

The failure of these controllers was not the result of a cyber attack. However, it demonstrates the effect that one component can have on an entire PCS network and every device on that network. Combined with the Davis-Besse worm infection, the Browns Ferry shutdown presents a possible attack scenario. If a worm like Slammer had infected the control network of an active plant and attempted to spread not only through UDP, but also through Ethernet, it could have disabled the recirculation pumps as well as the sensors that would alert plant personnel to the problem.

Hatch automatic shutdown

Due to the growing network connections between control systems and office computers, even seemingly simple actions can have unexpected results. On March 7, 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shutdown after an engineer applied a software update to a single computer on the plant's business network. The computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on both networks. When the engineer rebooted the computer, the synchronization program reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown.[23]

This innocent mistake demonstrates how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor—even if they have no intent to interfere with critical systems. This incident is probably the least critical of those examined so far, since it *activated* safety systems rather than disrupting them. However, it also demonstrates that plant operators do not fully understand the dependencies between network devices. This would make it difficult to identify and protect all the vulnerabilities in a process control system.

Stuxnet: a proof of concept

The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a sophisticated adversary with a detailed knowledge of process control systems can have on critical infrastructures. Stuxnet is believed to have destroyed 984 centrifuges at Iran's uranium enrichment facility in Natanz.[24] An analysis of the event by the Institute for Science and International Security (ISIS),

23 Brain Krebs, "Cyber Incident Blamed for Nuclear Power Plant Shutdown" *Washington Post*, June 5, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

24 William J. Broad, John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iranian Nuclear Delay". *New York Times*, January 15, 2011.

based on open source technical data about the Stuxnet computer worm and the Iranian nuclear program, found that Stuxnet may have been designed specifically for that purpose. However, Stuxnet also demonstrates the limitations that even such a sophisticated adversary would face in launching an attack against process control systems. The ISIS report finds that the Stuxnet attack, though it successfully disrupted the Iranian centrifuge program, did not slow down Iran's accumulation of low-enriched uranium.[25] The attack is remarkable for its sophistication, but it did not pose an epic threat to Iran.

However, that sophistication must be considered when assessing the vulnerability of nuclear facilities to cyber attack. The Stuxnet worm targeted specific PCS components used in the Iranian centrifuge cascades: a frequency converter manufactured by Iranian firm Fararo Paya, another frequency converter manufactured by Finland's Vacon,[26] and the S7-315 and S7-417 programmable logic controllers made by Siemens.[27] The PLCs controlled the frequency converters to modulate the speed at which the centrifuges spun. Stuxnet commanded the PLCs to speed up and slow down the spinning centrifuges, destroying some of them, while sending false data to plant operators to make it appear the centrifuges were behaving normally. The *New York Times* report suggests that Stuxnet's authors may have learned about vulnerabilities in the Siemens controllers thanks to a partnership between Siemens and the Idaho National Laboratory aimed at assessing vulnerabilities in such components. These products are general PCS components not unique to the Iranian nuclear program; Siemens reports that at least 24 of its customers were infected by Stuxnet, though they suffered no damage.[28]

The reason Stuxnet did not disrupt every vulnerable PCS it infected is that it was programmed to disrupt only systems that had the same configuration as the centrifuge cascade used at Natanz.[29] Antivirus company Symantec began detecting Stuxnet traffic in June 2009, mostly in Iran, but also in neighboring countries. However, since it did not spread aggressively and did not damage the systems it had infected, it raised little alarm.[30] Only at the Natanz enrichment facility did it have a major effect. Experts cited by the *New York Times* report suggest that Israeli intelligence provided the specific technical details necessary for Stuxnet to limit its damage to the Iranian nuclear program.

While the *New York Times* article only presents a possible scenario, that scenario and the evidence reflect the challenges of executing a catastrophic cyber attack against a nuclear facility. Programming is a cyclical process of trial and error. For an amateur hacker working only with a computer, the costs of testing software are trivial. Testing software designed for process control systems, however, requires access to the system in question, which is usually expensive. Malicious hackers could run tests on a remote PCS they had compromised, but an unsuccessful test could raise alarms or damage the system before the hackers were ready for the next stage of an attack. The Stuxnet authors would need a dedicated testbed to refine their code. Stuxnet also incorporated technical information specific to the Iranian facility. These resources are out of the reach of amateurs and would require

25 David Albright, Paul Brannan, and Christina Walrond. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report". ISIS Report, February 15, 2011, pg 2.

26 David Albright, Paul Brannan, and Christina Walrond. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment". ISIS Report, December 22, 2010, pg 3.

27 Albright, Brannan, and Walrond. "Stuxnet Malware", pg 1.

28 "SIMTAC WinCC / SIMTAC PCS-7: Information about Malware / Viruses / Trojan horses". Siemens, accessed April 14, 2011. http://support.automation.siemens.com/WW/llisapi.dll?query=stuxnet&func=cslib.cssearch&content=adsearch%2Fadsearch.aspx&lang=en&siteid=cseus&objaction=cssearch&searchinprim=0&nodeid0=10805583

29 Albirght, Brannan, and Walrond. "Stuxnet Mlaware", pg 1.

30 Broad, Markoff, and Sanger. "Israeli Test".

the kind of funding and actionable intelligence that comes from state sponsorship.

The Stuxnet attack also incorporates elements of the other three incidents examined in this paper. First, it disrupted the systems that monitored physical components, like the Davis-Besse worm infection. Second, it interfered with programmable logic controllers, like the Browns Ferry data storm. Third, it relied on there being some path from ordinary office computer to process control systems, as in the Hatch automatic shutdown. At the same time, the Stuxnet authors innovated on these features: Stuxnet did not simply disrupt sensor output, it faked it; it did not simply interfere with PLCs, it gave them specific instructions; finally, it did not rely on an internet connection to Natanz—it also traveled between computers on worker's thumb drives[31] and infected components destined for Natanz at their source in the Iranian chain of supply.[32]

Skeptics and alarmists can both use the Stuxnet attack to justify their positions. Alarmists can point to the vulnerability of PCS and its direct effect on Iranian national interests. However, skeptics can argue that the Stuxnet attack required specific knowledge of a particular facility and cannot be generalized to other systems, the same argument used by the Massachusetts Water Resource Authority. Further, the impact could hardly be described as catastrophic. However, it is important to look at the Stuxnet attack in the context of history. Cyber attacks have evolved from the work of amateurs and professional criminals into a serious endeavor for states engaged in international disputes. States have begun to use cyber attacks not just to gather intelligence or control information networks, but to damage physical infrastructures. While the damage is nowhere near a "digital Pearl Harbor", the trend is clear: states are actively pursuing cyber attacks as an instrument of foreign policy while advancing the technical know-how such attacks require.

Lessons

These four incidents hold important lessons for the cyber security of nuclear facilities and critical infrastructures in general. First, skeptics claim that PCS are immune from attack since they are not connected to the internet. However, the Davis-Besse incident shows that this is a misconception; even operators who try to monitor and protect every connection cannot be sure they know about all of them. Stuxnet even traveled on portable thumb drives to infect computers that were not connected to the internet. Second, skeptics argue that PCS are immune from attack since they are different from ordinary computers. However, all four incidents demonstrate that PCS have become interoperable with ordinary computers, making them vulnerable. Third, vulnerabilities are more complicated than both skeptics and alarmists realize. Alarmists often invoke the danger of hackers taking control of a power plant, but these incidents show how unintelligent computer viruses and even malfunctions in small devices can have big unexpected effects. This suggests that even though nuclear facilities are vulnerable to attack, a malicious hacker would have difficulty making sure an attack works precisely as planned. Even so, states are working make cyber attacks more precise, supplementing their methods with intelligence from other sources.

Cyber security and nuclear safety regulations

As states take a greater interest in launching cyber attacks against nuclear facilities, they should also

31 Albright, Brannan, and Walrond. "Did Stuxnet Take Out 1,000 Centrifuges?" pg 7.
32 Albright, Brannan, and Walrond. "Stuxnet Malware", pg 2.

take a greater interest in protecting their own facilities against attack. This means translating the lessons of previous incidents into workable guidance and regulation for plant operators. So far, this has been lacking, both from the United States government and the International Atomic Energy Agency (IAEA). The nuclear industry does not have the expertise to handle such threats on its own, as evidenced not only by the incidents covered here, but also by the lack of compliance with NERC critical asset identification standards.[33]

However, the agencies charged with providing the necessary guidance may not have that expertise themselves. The U.S. Nuclear Regulatory Commission (NRC) did not issue an Information Notice after the Hatch shutdown as it had for the Davis-Besse and Browns Ferry incidents. The NRC is aware of its expertise gap and is actively addressing it. In January 2008, the NRC's newly established Computer Security Office launched a working group to develop an Information Security Strategic Plan (ISSP) for 2010 to 2015. The working group found that cyber security issues at nuclear plants were handled in an "ad hoc" manner, since the NRC's staff with cyber experience were both limited and widely dispersed about the country. The NRC set up an Information Security Steering Committee to coordinate the activities of these dispersed experts under the ISSP, including the development of new rules and regulatory guidance for cyber security at nuclear facilities. Part of that process will be implementing a 2008 recommendation from the Office of the Inspector General to develop a program of cyber security inspections at nuclear power plants.[34] The ISSP outlines plans to use the NRC's licensing and inspection authority to enforce cyber security standards at nuclear facilities,[35] however, it is too early to judge the effectiveness of these efforts.

While the IAEA lacks the enforcement powers of the NRC, it still has an important role to play as inspector and advisor to the nuclear programs of other nations. However, it seems to be a bit slower than the NRC in developing its cyber security expertise. Its most recent technical guidance on the matter seems to be "Security of Information and Instrumentation & Control Systems at Nuclear Facilities" released in 2007. However, this guidance fails to account for documented PCS incidents in both nuclear and non-nuclear facilities and the reported experience of penetration testers. For example, the guidance states that cyber security at nuclear facilities can be achieved using the same methods and tools developed for IT security.[36] However, the Browns Ferry data storm was created by either a failed PCS component or normal network operations; IT security would not have predicted the resulting failure of the reactor pump VFDs. Since then, Stuxnet has further demonstrated the inadequacy of basic IT security, since it infected PCS components in the Iranian supply chain rather than looking for a direct network connection to Natanz. The guidance also recommends developing a network diagram documenting all external connections, however, the assumption that all external connections were known and controlled was the basis for the supposed invulnerability of PCS. Even in the IT world, penetration testers have found that network diagrams are often grossly inaccurate and only create a false sense of security. While the IAEA guidance does give some sound advice for basic cyber security, it does not begin to address the unique challenges presented by PCS. The IAEA is continuing to develop its expertise in this area, especially since the Stuxnet attack, however, the current state of official guidance and regulation suggests that those responsible for protecting nuclear facilities from cyber attack are less prepared than their potential

33 Assante. "Critical Cyber Asset Identification".

34 Stephen D. Dingbaum. "NRC's Planned Cyber security Program (OIG-08-A-06)". Memorandum Report from the Office of the Inspector General (March 18, 2008).

35 Nuclear Regulatory Commission, "Information Security Strategic Plan". May 18, 2009. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2009/secy2009-0077/enclosure.pdf

36 International Atomic Energy Agency. "Security of Information and Instrumentation & Control Systems at Nuclear Facilities", *IAEA Nuclear Security Series No. XX Technical Guidance*. 2007, page 13.

aggressors.

Conclusion: A mixed bag

While some cyber security incidents have occurred at nuclear power plants, crossing the imaginary boundary between IT and PCS and shutting down reactors, so far the potential for damaging a nuclear reactor appears theoretical. Scott Lunsford, a penetration tester for IBM, says government mandated safeguards would prevent a hacker from triggering a meltdown. So far, no catastrophic damage has resulted from a cyber attack against a nuclear facility. The same cannot be said for other sectors, as in the case of the Maroochy water incident, and the Stuxnet attack has demonstrated that states are likely pushing the development of new tactics and capabilities in cyberspace.

Although the experience of the nuclear sector lags behind that of non-nuclear facilities in cyber security and PCS, nuclear plants must also comply with stronger safety regulations and inspections. Although he NRC's cyber regulations are still being developed, its existing regulations have put several incidents on the public record that would have gone unreported by non-nuclear power plants. This parallels the trend of cyber security in e-commerce. In the early 2000's, banks and online merchants commonly suffered cyber attacks that potentially revealed their customers private data to hackers. To protect their reputations, they hired consultants to quietly fix their systems under a non-disclosure agreement. Eventually, California passed SB1386, requiring any company that did business in the state of California to notify their customers if a hacker could have potentially accessed their private data. After the law went into effect in July 2003, the extent of the hacking became public knowledge and companies began to invest in cyber security to reassure their customers before they suffered an attack. Oil, gas, and electric companies have been active in protecting their PCS from cyber attack, however, they still have little incentive to report the attacks they suffer. No regulation requires it, and companies fear their information could be made public under the Freedom of Information Act if they do. The years from 2010 to 2015 could prove decisive in the field of PCS security. If the NRC can implement the same sort of rigorous inspection and reporting requirements for cyber security as they have for physical security and safety, it may open the field up to greater public scrutiny and spur the investment needed to better protect critical infrastructures.

About the Author

Brent Kesler graduated from Dartmouth College in 2003 with a degree in computer science. Until 2006 he wrote *Security in the News*, a daily report of developments related to malicious hacking, malware, cyber security best practices, and homeland security. He later worked as research coordinator for the Institute for Information Infrastructure Protection (I3P), helping manage federal research projects related to critical infrastructure protection. In 2010, Mr. Kesler graduated from the Monterey Institute of International Studies, building on his cyber security background with a master's degree in international policy and a focus on terrorism.

Cyber Conflict Between Taiwan and China

Yao-chung Chang

Introduction

The Republic of China (Taiwan hereafter) and the People's Republic of China (China hereafter) are two particularly attractive targets for internet hackers. Reports have found that, compared to other countries in the Asia and Pacific regions, China and Taiwan rank as the top two countries in terms of malicious computer activity.[1,2] Reports have also shown that most hacking into Taiwanese computer systems is initiated from within China and most hacking into Chinese systems originates within Taiwan.[3,4,5,6,7]

Malicious computer activity across the Taiwan Strait not only impacts computer users in Taiwan and China but it also affects numerous users in other countries as well. It is not only a problem for China and Taiwan to remedy, nor is it one that they alone should deal with. As a matter of fact, reports have found that there have been a number of computer attacks against the US that originated from computers in Taiwan but were controlled by command and control servers in China.[8]

The current lack of formal mutual cooperation between Taiwan and China has become a bottleneck for the successful investigation of transnational cybercrime. Therefore, the establishment of other feasible mutual cooperation options between Taiwan and China has become an important concern not only between Taiwan and China but for all countries.

Impeded by the present political situation, there is currently no formal mutual assistance agreement against crime between Taiwan and China.[a] However, there exists a level of quasi-formal and informal cooperation between law enforcement agencies, and these include "the Kinmen Agreement", "the Agreement on Cross-Strait Mutual Assistance in Crime Matters" (hereafter, the Agreement on Mutual Assistance), and informal police-to-police cooperation. It is arguable whether these existing cooperation methods are applicable to cybercrime issues because cybercrime is potentially more sensitive for both governments as opposed to more conventional crimes.

This paper will introduce cases of cybercrime across the Taiwan Strait and the existing mutual cooperation methods used against crime. Based on interview data, it will also examine the use of quasi-formal agreements signed by non-governmental organizations under the authorization of both governments, and it will then examine the role played by informal relationships between police officials. In each case, the paper will examine obstacles these strategies face in obtaining cooperation.

◆ ◆ ◆

[a] The Government of People's Republic of China (China) claims sovereignty over Taiwan. Consequently, there is no possibility for Taiwanese and Chinese governments to sign a formal mutual agreement. For the special political situation between Taiwan and China, see Chapter 7 of *The Republic of China Year book 2009, Cross-strait Relations* at http://www.gio.gov.tw/taiwan-website/5-gp/yearbook/06Cross-straitRelations.pdf.

Methodology

Thirty-eight interviews (including four focus groups, one in China and three in Taiwan) with a total of 44 interviewees were conducted in Taiwan and China during the years 2008 and 2009. All the interviewees interviewed in Taiwan are coded with the letter "T" while those in China are coded with the letter "C". The number following the letter refers to the case record. For example, T001 means the first interview done in Taiwan.

Interviewees were selected purposely based on their work experience or background. People with knowledge of information security and cybercrime were potential samples for this research. These included but were not limited to IT people in government agencies and private companies, police officers, prosecutors, and other professionals in cybercrime and information security, such as professors, managers of legal compliance in companies, and information security experts in big accounting firms which audit information security and conduct staff training in organizations. They were categorized into four groups: public sector, private sector, law enforcement, and other professionals.

The concept of data saturation, whereby data is collected until no new information is obtained,[9] was adopted by this research as the basis to decide the sample size. Except for the interviews in the categories of public sector and law enforcement agencies from China, interviews in other categories all reached the point of theoretical saturation.

In Taiwan, there were 23 interviews with 28 interviewees. There were only three interviewees with less than ten years experience in information security or related areas. All other interviewees in Taiwan had more than ten years working experience in this area. Four participants were female.

Among all the interviews in Taiwan, ten were conducted with 12 participants from the private sector; five interviews were conducted with seven participants from the public sector; four interviews were conducted with five participants from law enforcement agencies such as the police and prosecutors; and four professors were interviewed who were experts in law, information security issues or criminology.

In China, 15 interviews were conducted and 16 people participated. Seven interviews were conducted with eight participants from the private sector; three policemen were interviewed as well as five professors. With regard to the experience levels of the interviewees in China, only two had experience in the related area of less than ten years. In terms of gender, only one interviewee was female.

There were no Chinese government agencies willing to be interviewed. As well, there were no Chinese prosecutors interviewed. However, in lieu of formal prosecutors, some professors interviewed were also concurrently serving as deputy chief procurators. Their contributions helped overcome the lack of data from government officers and prosecutors in China.

Cases of Cybercrime Across the Taiwan Strait

The special political situation between Taiwan and China, and their often antagonistic relationship, has encouraged the growth of malicious activities between them. It has been reported that both Taiwan and China possess net-armies which hack into their respective counterpart government systems to conduct cyber espionage and to steal sensitive data.[10,11,12] Additionally, websites of a

sensitive political nature, such as those criticizing the "one China policy" are usually prime targets for distributed denial of service attacks (DDoS). [b]

As an example, a significant number of cyber attacks occurred in 1999 when a special state-to-state relationship was declared by then-President of Taiwan Teng-hui Lee. In that year President Lee declared in an interview with *Deutche Welle* that relations between Taiwan and China were of a state-to-state nature, or at least a "special" state-to-state relationship existed. Seeing that interview as a possible pro-Taiwanese independence declaration, nationalistic Chinese hackers cracked into Taiwan's government websites to show their anger. Government websites such as those belonging to the Administrative Yuan, the Control Yuan, the National Assembly, and Presidential Executive Office were replaced with an image of the Chinese five-star flag and with political statements such as "Taiwan is an indivisible part of China". As revenge, Taiwanese hackers spontaneously responded in kind. They hacked into Chinese government websites and replaced the image of China's national flag with the Taiwan national flag.[13,14]

This example is not isolated and similar events occur often. In 2002, a website constructed by the "Taiwan Tea Party", which supports the independence of Taiwan, suffered consistent and serious DDoS which paralyzed its operation. A huge quantity of spam and messages from China was sent to the website, shutting it down (Chen 2002).[15] In 2005 and 2006, Taiwan's Ministry of National Defense was hacked into and computers in the Minister's Office and the Secretary's Office were infected with trojans and spyware.[16] The Acting Director of the National Security Bureau in Taiwan has said that a Chinese cyber army launched more than 3,100 attacks against Taiwanese government systems in 2008, and this does not include attacks against the private sector. Their purpose was mainly related to stealing data and sensitive information.[17]

However, not all cyber attacks across the Taiwan Strait have political motivations. Some hackers do it simply for revenge, fun, or profit. For example, Shau et al. (2005) has suggested that at least 60 per cent of the cybercrime occurring in China is financially motivated.[18] Among all targets, banks, the stock market and other financial agencies are the main victims. A senior police officer mentioned that the website of his institute was once hacked into and a Chinese national flag (usually called the "five star flag' in Taiwan) was inserted on the main page, showing off the hacker's ability to hack into government agencies (T017).

Existing cooperation models against crime

Although there is no inter-governmental mutual assistance agreement between Taiwan and China, there are two agreements signed by non-governmental organizations with government support or authorization. One is the agreement in relation to extradition, the Kinmen Agreement, which was signed by the Red Cross Society of the People's Republic of China and the Red Cross Society of the Republic of China with support from both governments. The other is the Agreement on Cross-Strait Mutual Assistance in Crime Matters. It was signed in 2009 between the Taiwan-based Straits Exchange Foundation (SEF), and the mainland-based Association for Relations Across the Taiwan Straits (ARATS).

[b] A *distributed denial of service* (DDoS) attack makes web sites or other network services unavailable to users by flooding the resource with spurious requests from many computers.

As a framework for the swift repatriation of stowaways and criminals, the Kinmen Agreement on Handling Deportation of Wanted Criminals and Suspects was signed in 1990 between the Red Cross Society of the People's Republic of China and the Red Cross Society of the Republic of China (Taiwan). This was the first bilateral agreement between Taiwan and China since 1949, although both governments did not sign it but authorized non-governmental organizations to sign. It was also the first document between the two countries to contain "quasi-judicial" mutual assistance provisions and is recognized as a precedent for the Agreement on Cross-Strait Mutual Assistance in Crime Matters.[19]

The Agreement contains provisions for the repatriation of individuals who have illegally entered either country, as well as repatriation of criminals and suspects. Although it is concerned mainly with the repatriation of certain categories of people, it does imply cooperation between Taiwan and China in the arrest of criminals and suspects. According to informal statistics, between 1990 and January 2009, more than 38,000 persons who had fled to China were repatriated, including some serious criminal offenders.[20]

Immediately following the signing of the Kinmen Agreement, the Straits Exchange Foundation[c] was established in Taiwan in November 1990 and the Association for Relations Across the Taiwan Straits[d] was established in China in December 1991. These two non-governmental organizations, both authorized by their respective governments, have become the main channels for official communications between Taiwan and China. In 2009, the Agreement on Cross-Strait Mutual Assistance in Crime Matters was signed by these two organizations. That agreement is recognized as a milestone in cooperation against crime between Taiwan and China.

Containing 24 articles in five chapters, the Agreement covers the extent of cooperation, the types of crime covered, mutual assistance in crime investigation and evidence collection, and other administrative aspects. Unlike the Kinmen Agreement, which focuses on the repatriation of criminals or suspects, this agreement focuses on collaboration in combating crime and the arrest of criminals.

Mao-Su Huang,[e] the Deputy Director-General of Taiwan's National Police Agency,[f] comments that the Agreement has institutionalized collaboration in combating crime.[21] Positive comments were also made by a spokesperson for the Taiwan Affairs Office of the State Council of the People's Republic of China at a news conference held in December 2009:

> The Agreement realized the institutionalisation, generalisation and comprehensive nature of the judicial mutual assistance across the Taiwan Strait. Since entering into effect in June, it is executed very well with significant outcomes. It promoted greatly the efficiency of collaboration between both sides, and protected the rights and interests of citizens on both sides.[22]

Not surprisingly, there has been criticism of the Agreement on Mutual Assistance. Some commentators think that both sides have been too optimistic when praising its benefits. Tong (2009) doubted that China would extradite criminals and suspects under the new Agreement because China did not always send criminals back under the previous Kinmen Agreement. He noted that China refused to repatriate stowaways under the Kinmen Agreement for a certain period of time when the relationship between Taiwan and China was tense.[23]

---

[c] 海峡交流基金會

[d] 海峡两岸关系协会

[e] 黃茂穗

[f] He was commissioner of the Crime Investigation Bureau when the Agreement was signed.

Chang (2010) also advised that although some requests had been made by Taiwan, "they are still pending and the attitude of the Chinese Government in terms of cooperation is the most important factor." He said, in an interview with Taiwanese Government officials, that trust between Taiwan and China is the key to the success of the Agreement. Therefore, the effectiveness of the Agreement on Mutual Assistance is still hugely reliant on the political situation between, and the attitudes of, both Taiwan and China—especially the attitude of China.[24]

Informal police-to-police cooperation

Apart from the above quasi-formal agreements against crime, informal police-to-police cooperation is often used to advance crime investigations. Some senior police and academics said that limited mutual help with investigations has been secured privately and that some *guan-xi* (關係 "informal relationships") exist between the police in Taiwan and China.

Guan-xi, which resembles the idea of social capital, plays a very important role in different aspects in Chinese society.[g] As Yang notes in her anthropological work on Chinese culture, the term *guan-xi* literally means relationship. However, she argued that in the context of the gift economy, "it has the sense of social connections, connections which must be carefully initiated, preserved and renewed through the giving and receiving gifts, favors and dinners or banquets."[25] It can be built on pre-existing relationships such as classmates, people from the same native-place, relatives, superiors and subordinates in the same working place and so on.[26]

G*uan-xi* between people also represents the trust between them. Based on *guan-xi*, police from both sides can build *mo-chi* (默契 "unspoken consensus") that facilitates crime investigation across the Taiwan Strait. As a senior investigator said, even under the political barrier, some crime problems still need to be cleared and this informal police-to-police relationship can help solve the problem:

> Many things can be done privately and not be discussed formally. It is related to the status of Taiwan. We think this is the most troublesome thing to us…It is just like the *mo-chi* between you and me. We know our "bosses" are like aliens to each other, but in order to achieve outcomes, we need *mo-chi* (T017, senior police officer).

A senior law enforcement officer in Taiwan also illustrated the existence of informal police-to-police relations and cooperation between Taiwan and China. He said that some police in the Crime Investigation Bureau in Taiwan had some *guan-xi* with the public police in China. They could deal with some cases "under the table". That is, there is some unofficial cooperation.

For example, in 2005 a cross-Strait kidnapping case was cleared with the help of informal police-to-police cooperation. While there was no formal mutual cooperation between Taiwan and China, the police in Taiwan, in order to solve the case, used their personal relations (*guan-xi*) to request help from police in China. The criminal was finally arrested by police in Macao and was sent back to Taiwan. Interestingly, official press releases do not emphasize this informal police-to-police relationship as it might be criticized for being "under the table".

---

[g] There are doubts about the similarity and differences of *guan-xi* and social capital, especially in the field of anthropology, where some argue that *guan-xi* is an essential and defining elemental part of Chinese culture, while others believe that *guan-xi* is little more than a Chinese word for social capital which can be found in all societies, see more discussion at e.g. Gold, Guther, & Wank (2002), Jacobs (1979), King (1991), Smart (1993), Yang (1988). Here, the original expression *guan-xi* is used to avoid any misunderstanding that might result from using other terms, such as "social capital".

Inevitably, there are some defects that diminish the effectiveness of informal police-to-police cooperation. One is that *guan-xi* is usually exclusive to the persons who build it and it does not usually last long. It is difficult to pass to others. Therefore, *guan-xi* might not work if the person changes position or leaves his job. Furthermore, informal police-to-police cooperation is still highly dependent on a positive political environment for *guan-xi* to be effective. In other words, if the relationship between Taiwan and China improves, the police may be able to achieve more. Equally, if the relationship between the countries worsens then little will be achieved.

Cooperation against cybercrime across the Taiwan Strait

From the discussion above, we can see that a number of alternate forms of cooperation against crime exist to cover the current lack of formal cooperation between Taiwan and China. These include quasi-formal mutual cooperation and informal police-to-police cooperation.

Theoretically, quasi-formal cooperation agreements, such as the Kinmen Agreement and the Agreement on Mutual Assistance should be sufficient for Taiwan and China to cooperate in combating cybercrime. This is supported by most of the interviewees. All elements for cooperation against cybercrime, such as mutual assistance in crime investigation and evidence collecting, and extradition, are included in these two agreements. Academics, both in Taiwan and China, believed that the agreements should be able to be used as a model for cooperation against cybercrime.

Elements of cybercrime, such as hacking and other malicious activities, were proposed for inclusion in the Agreement on Mutual Assistance by the Taiwanese negotiators.[27] However, cybercrime received no special mention in the final document. This may have been because cybercrime was not seen as a first order issue or that it was too sensitive for governments to address explicitly.

However, should attitudes change, the use of the generalized term "other crimes" in the Agreement on Mutual Assistance could cover cooperation on cybercrime for those cybercrimes which are not sensitive, such as purely economic crimes like fraud. Indeed, some cybercrime cases have been pursued under the agreements. For example, since the signature of the Agreement on Mutual Assistance, at least 100 computer fraud crime groups have been investigated and hundreds of criminals and suspects involved in computer fraud have been arrested.[28]

Although the agreements seem to enable Taiwan and China to cooperate when combating cybercrime, a police officer in China argued that it was a time-consuming and complicated process (C008). This is an understandable position. For example, the Agreement on Mutual Assistance is unclear as to which agencies have charge of the investigation and collection of evidence. In accordance with the text of the agreement, it seems that all requests need to be made between ARATS and SEF through assigned contact points, and those requests must be made in writing. This inevitably causes delay in the investigation and evidence collection.

Apart from the quasi-formal agreements listed above, informal police-to-police cooperation is another channel for cooperation when investigating cybercrime across the Taiwan Strait. As advised previously, a level of *guan-xi* already exists between certain police officers in China and Taiwan, leading to informal cooperation on major crimes. As a senior police officer said, for computer fraud cases, they cooperate "under the table" first in crime investigation and evidence collection. Through the use of *guan-xi*, they can ask "their friends" to locate criminals so that they can obtain accurate information on the criminal's whereabouts. When the case is ready to close, they will then formally apply for mutual assistance to the appropriate contact officer in charge of the region and seek the

arrest of the suspect criminals. This approach is more efficient than simply sending out a request to ARATS without any helpful background information.

Notwithstanding some success in this mutual assistance against cybercrime, the methods used have been limited and only apply to certain types of cybercrime. Most police interviewed were still very pessimistic about cooperation between China and Taiwan against cybercrime.

A senior police officer in China said that they seldom dealt with transnational crime cases, and if a case was related to Taiwan, there was even less chance of it being pursued. Similarly, some senior law enforcement officers in Taiwan said that, according to their experience or their understanding, when a crime originated overseas the local police could usually do "nothing":

> For Taiwan and China, zero. There is no mutual help between Taiwan and China. We try to tell them and ask for their help, but … basically there is no response (T004, senior police officer).

T004, a senior police officer in Taiwan, explained that this might be because some hackers were hired by their respective governments. Cooperation when combating cybercrime, especially when that cybercrime was directed against government agencies, was likely to be awkward even when both sides trust each other. As Professor Susan Brenner[h] indicated in her book *Cyberthreats: The Emerging Fault Lines of the National State*, it is quite impossible for the sponsoring state to cooperate in the investigating efforts:

> When what is ostensibly cybercrime is state-sponsored - as is increasingly true of economic espionage - the efficacy of the civilian law enforcement response process breaks down. The sponsoring state will almost certainly refuse to cooperate with the investigative efforts of the victim state's law enforcement officers, and thereby thwart the crime response process.[29]

Apart from government-sponsored crime, it was also argued by interviewees that it was highly improbable that governments would cooperate when investigating "hacktivism" which supports their own national interests. For example, if an attack against a Taiwanese website originated in China, and that website specifically opposed China's "one China policy", it can be safely predict that neither Taiwan nor China would offer much cooperation when investigating that matter. The case of the attack against the official website of the 2009 Kaohsiung Festival, which screened The *Ten Conditions of Love,* a documentary about exiled Uighur activist Rebiya Kadeer, is a good example.

Given this, the Chinese and Taiwanese governments could only be anticipated to cooperate if it could be shown that the hackers involved were not supported by either government or that the hacking behavior was not related to national interests. Senior police officers in Taiwan believed that cooperation against cybercrime between Taiwan and China was possible if it was an economic issue and there is no government element involved and when both sides suffered from the same crime:

> …Only when they are suffering from the same crime do they cooperate. Do you remember the news not long ago about organised crime being cleared-up? That group not only committed fraud in Taiwan, but also in China. That is why China's public police were willing to help. See, I reckon only when they are suffering will they help! (T017)

> When the Chinese suffer from the same crime will they start to cooperate? The best example of cooperation is the mutual assistance between Taiwan and China in terms of telecommunication and computer fraud! (T004)

[h] NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law.

In addition to the nature of the cybercrime being committed, the political situation between Taiwan and China can determine whether cooperation is possible. Most interviewees agreed that there would be no cooperation between Taiwan and China when the political situation was tense. T017 said that, when Cross-Strait relations were tense, Taiwan could hardly get a response from China to their requests. Even informal police-to-police cooperation stopped—even *guan-xi* does not work when relations between Taiwan and China are bad.

The attitude of the respondent can also play a vital role in cooperation. According to a senior police officer's experience, most of the SEF requests to ARATS for help in cybercrime investigations remain unsettled. Often only a *pro forma* reply to the request for assistance was received, even when the relationship was good:

> I remember that we had requested ARATS, via SEF, to investigate some cybercrime problems. For most of the cases, we did not get any response from them. Even if there was a reply, the answers were usually pro forma, telling us that they could not find any information or there was nothing wrong (T017).

Conclusion

It is encouraging that, despite the lack of formal mechanisms for mutual assistance between Taiwan and China, there are alternative channels for cooperation, including quasi-formal mutual assistance and informal police-to-police cooperation. Current agreements and informal police-to-police cooperation could potentially be sufficient for police from both sides to cooperate with their counterparts against cybercrime. However, that cooperation can only apply to cybercrimes that are purely economic in nature and where there is no government involvement. Cooperation is more likely when both countries are suffering from the same crime, such as computer fraud.

There are still barriers impeding cooperation between the two countries. Cooperation, whether quasi-formal or informal, is highly dependent on the official or governmental relationship between Taiwan and China existing at the time of the criminal investigation. Quasi-formal cooperation and informal cooperation through *guan-xi* between police forces work well only when the official relationship between Taiwan and China is not tense. Moreover, as indicated by interviewees, the attitude of respondents can also potentially impede cooperation.

It may be a long time before the two governments are able sign an official agreement for formal mutual assistance against cybercrime. However, with current improvements in the relationship between Taiwan and China, there is optimism that the situation could change in the near future. In the interim, and in the absence of a formal agreement, it is all the more important to advance the current quasi-formal and informal cooperation between Taiwan and China.

About the Author

Dr. Yao-chung Chang completed his PhD at the Centre of Excellence in Policing and Security, Regulatory Institutions Network, at the Australian National University. His PhD research, entitled "Cybercrime Across the Taiwan Strait: Regulatory Responses and Crime Prevention," focuses on alternative solutions to combating cybercrime during a period of negative mutual assistance between both China and Taiwan. He is now working as a research officer at the Centre of Excellence in Policing and Security.

In 2005-2007, he worked as a researcher and project manager at the Science and Technology Law Centre, Institute for Information Industry, which is recognized as one of the most important think tanks for the Taiwanese Government in the area of legal responses to new technology.

Notes

[1] Symantec. *Symantec APJ Internet Security Threat Report XII: Trend for January-June 2007*, edited by D. Turner. Cupertino, CA: Symantec Corporation, 2007.

[2] Symantec. *Symantec APJ Internet Security Threat Report XIII: Trend for July-December 2007*. Cupertino, CA: Symantec Corporation, 2008.

[3] Mazanec, Brian M. "The art of (cyber) war", *Journal of International Security Affairs* Spring 2009. Accessed September 18, 2010. http://www.securityaffairs.org/issues/2009/16/index16.php.

[4] Schneier, Bruce. "The Truth About Chinese Hackers" Discover Channel's *Discovery Tech* blog. 2008. Accessed September 18, 2010. http://dsc.discovery.com/technology/my-take/computer-hackers-china.html

[5] Zhang, H. Y. "Taiwanese net-armies are targeting China", *People*, November 1, 2007.

[6] "Hackers Tap Wen's Work Report", Boxun News. March 31, 2009. http://www.boxun.us/news/publish/chinanews/Hackers_Tap_Wen_s_Work_Report.shtml

[7] Crime Investigation Bureau. "Taiwanese hackers, cooperating with Chinese hackers, hacked into banking systems in Taiwan". June 9, 2004. Accessed September 20, 2010. http://www.cib.gov.tw/news/news01_2.aspx?no=419.

[8] Rohozinski, R. D. Rafal, ed. "Tracking GhostNet: Investigating a Cyber Espionage Network", Toronto: Information Warfare Monitor, 2009.

[9] Morse, Janice M. "The significance of saturation." *Qualitative Health Research* 5 (1995): 147-149.

[10] Mazanec. "Art of (cyber) war".

[11] Schneier. "Truth About Chinese Hackers".

[12] Zhang. "Taiwanese net-armies".

[13] Hu, Y. C., and J. C. Lin. "Cyberwar across the Taiwan Strait", *China Times*, August 10, 1999.

[14] Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* McLean: Northrop Grumman Corporation, 2009.

[15] Chen, T. Z. "Taiwan Tea Party website attacked by DDoS", June 13, 2002. Accessed September 18, 2010. http://www.pczone.com.tw/vbb3/archive/t-47652.html

[16] Huang, J. P. "Chinese Net-army again stormed the Ministry of National Defence". *Apple Daily*, May 15, 2006.

[17] Xu, S.C. "Over 3,100 cyber attacks towards Taiwanese Government System were originated by Chinese cyber army". *Liberty Times*, March 24, 2009.

[18] Shau, J. M., B. H. Yu, R. Huang, L. J. Wong, H. J. Jheng, S. P. Jou, and J. T. Wong. *The Evolution of Crime*. Beijing: Peking University Press, 2005.

[19] Chen, R., and J. S. Wang. "From the Kinmen Agreement to the Agreement on Cross-Strait Mutual Assistance in Crime Matters". *Fu-Jen Law Journal* 99:51-55, 2009.

[20] "38,936 persons have been repatriated under the Kinmen Agreement". *Sina News*, Februrary 10, 2009.

[21] Jen, M. H. "Mutual assistance between Taiwan and China. C.I.B.: Institutionalised the collaboration of combating crime". *Central News Agency*, April 26, 2009.

[22] Lee, H. F., and J. H. Wu. "Judicial mutual assistance safeguards the rights and interests of citizens on both sides". *Xinhuanet*, December 29, 2009.

[23] Tong, W. S. "An analysis on the judicial agreement between Taiwan and China". *Epoch Times*, May 3, 2009.

[24] Chang, G. L. "Mutual assistance between Taiwan and China: It is still difficult to repatriate criminals". *China Times*, January 3, 2010.

[25] Yang, Mayfair M. "The modernity of power in the Chinese socialist order". *Cultural Anthopology* 3 (1988): 411.

[26] Ibid.

[27] Jiang, J. Y. "Issues of Hacking and Extradition will all be included in the Jiang-Chen Meeting". *Haixia Info*, March 31, 2009.

[28] "Great success on mutual assistance against crime matters". *China Review News*, September 15, 2010.

[29] Brenner, Susan. *Cyberthreats: The Emerging Fault Lines of the National State.* (Oxford: Oxford University Press, 2009), 97.

Works cited in footnote g:

Gold, Thomas, Doug Guthrie, and David Wank. "An introduction to the study of guanxi". *Social Connections in China: Institutions, Culture, and the Changing Nature of Guanxi*, edited by T. Gold, D. Guthrie and D. Wank. Cambridge: Cambridge University Press, 2002.

Jacobs, J. Bruce. "A preliminary model of particularistic tie in Chinese political alliance: Kan-ch'ing and kuan-hsi in a rural Taiwanese township". *The China Quarterly* 78 (1979): 237-273.

King, Ambrose Yeo-chi. "Kuan-hsi and network building: A sociological interpretation". *Daedalus* 120 (1991) 2: 63-84.

Smart, Alan. "Gift, bribes, and guanxi: A reconsideration of Bourdieu's social capital". *Cultural Anthropology* 8 (1993) 3:388-408.

The Situation is Under Control

Cyberspace situational awareness and the implications of China's internet censorship

Robert Sheldon[a]

I. Introduction

Just prior to his confirmation as Commander of US Cyber Command (USCYBERCOM), General Keith B. Alexander identified the need to improve cyberspace situational awareness as one of his central responsibilities—and challenges.[1] This mission is rooted in the need to monitor computing activities across the 15,000 networks and seven million devices that compose the Department of Defense (DoD) information and communications technology (ICT) enterprise.[2] Complicating this mission further, USCYBERCOM must also conduct offensive operations in cyberspace and potentially assist the Department of Homeland Security's (DHS) efforts to defend other information systems across the federal government and US critical infrastructures.[3] These demands help explain what a Defense Information Systems Agency official recently called DoD's "insatiable desire for situational awareness" in cyberspace.[4]

Unfortunately for those who would seek to assess USCYBERCOM's progress, no "gold standard" exists for cyberspace situational awareness. It remains challenging to envisage the bounds of future situational awareness capabilities, let alone performance metrics. Thus, analyzing the present state of cyberspace situational awareness for a potential competitor yields a richer understanding of the relative US position. China serves as a sensible counterpart in this comparative analysis for several reasons. Some cite China as a potential military competitor[5] and future conflicts appear poised to spill into (if not originate in) the cyber domain.[6] China's military, moreover, has a well-documented offensive cyberwarfare doctrine that in some respects appears directed toward the United States.[7]

In parallel, China conducts sometimes "pervasive" internet censorship as part of "one of the largest and most sophisticated filtering systems in the world," according to the OpenNet Initiative.[8] Policymakers traditionally view internet censorship as a human rights issue.[9] In the past year, however, several technology companies have cogently argued that censorship also acts as a barrier to trade.[10] This article complements these views with a discussion about internet censorship's security-related implications. Specifically, this analysis argues that some of China's internet censorship techniques likely improve that nation's cyberspace situational awareness—which could affect the outcome of a conflict in cyberspace.[11]

This argument advances in section II with an explanation of some key concepts. Section III provides a brief survey of the development and state of cyberspace situational awareness within the United States. Sections IV and V, respectively, explain some key features of the cyber domain in China and gauge their impact for cyberspace situational awareness. Section VI identifies some inherent tradeoffs in the composition of the cyber domain in China. Section VII offers some conclusions and implications for US policymakers.[12]

---

[a] This paper presents the author's personal views and does not reflect those of any institution with which he is affiliated. The author wishes to thank Edward Monan and several anonymous reviewers, whose thoughtful comments on previous drafts helped to greatly improve this paper.

II. Definitions and key concepts

Internet censorship

For the purposes of this analysis, "internet censorship" is any measure enacted to restrict internet accessibility, processes, functions, or content based on sociopolitical imperatives. Such efforts take place in four distinct realms: laws and regulations; norms; markets; and architecture.[13] This paper emphasizes the architectural component, which has the most direct implications for situational awareness. The term "architecture" refers to the physical dimension of cyberspace, described in the *National Military Strategy for Cyberspace Operations* as "information systems and networks, computers and communications systems, and supporting infrastructures."[14] Architecture also encompasses network design and layout and the nature of connections with other networks, including those beyond national borders.

States can conduct censorship at four key architectural layers. These include, from least to most centralized: individual computers, organizations, internet service providers (ISPs), and the internet backbone.[15] China has generally succeeded in exerting control at each of these four layers. For example, at the individual layer, Tencent's popular instant messaging software QQ incorporates a client-based keyword-blocking utility.[16] At the organizational layer, China requires all internet content providers, such as websites, to gain licenses and comply with censorship mandates.[17] China "outsources" some censorship responsibilities to ISPs, the third architectural layer, which must police domestic internet content and enforce website closures.[18] Finally, this article centers on China's robust filtering activities at the internet backbone layer, specifically at gateways between Chinese networks and the rest of the internet.[19]

Cyberspace situational awareness

The Department of Defense (DoD) has no official, unified definition for "cyberspace situational awareness,"[20] despite the term's frequent, government-wide usage since the mid-2000s.[21] The 2006 National Military Strategy for Cyberspace Operations, however, sufficiently describes the concept:

> Cyberspace situational awareness enables commanders and planners to assess the current situation, collaborate on courses of action, take action, and anticipate opportunities and challenges in the domain. Automated tools must be employed to provide near-real time notification of anomalous activity and properly inject appropriate data into operational views to characterize the cyberspace activity. This situational awareness combined with proper risk assessments, including intelligence loss or gain determinations, will allow commanders to make the best decisions on courses of action.[22]

An important distinction must be made between *enterprise situational awareness* and *domain situational awareness*.[23] Enterprise situational awareness is visibility of the events and activities within a single entity's networks. This capability would, for example, enable informed computer network defense operations. However, defense against a large-scale, coordinated cyberattack targeting government, private industry, and privately owned infrastructures would require some level of situational awareness across multiple entities. Thus, domain situational awareness is visibility of events and activities spanning national (and ideally international) networks. This analysis addresses certain enterprise-level issues, but focuses on the domain level.

◆ ◆ ◆

III. Cyberspace situational awareness in the United States

Policy

In many aspects of the cyber domain, particularly those that relate to computer network attack, US capabilities appear far more advanced than the policies that guide their use. This resembles the early phases of the nuclear age, prior to the advent of deterrence theory and other guiding concepts.[24] Situational awareness is one of the few elements of the cyber domain where policy is more fully developed than enabling technologies and capabilities (discussed below). Several official documents and statements indicate the US government's policy: more is better.

With respect to enterprise situational awareness, the 2011 US budget states that the Office of Management and Budget should initiate ICT programs and activities that promote the "[m]ove towards Situational Awareness across the Government". The document asserts that:

> More frequent reporting, near or at real-time, is imperative for developing situational awareness across the Federal enterprise. The use of Security Information Management or Security Information Event Management tools will assist in progressing towards real time security awareness and management in the Government.[25]

This echoes two components of the US Comprehensive National Cybersecurity Initiative (CNCI). One specific initiative is to "[d]eploy an intrusion detection system of sensors across the Federal enterprise." This project aims to bolster the US Computer Emergency Readiness Team's (US-CERT) situational awareness so it can better develop and distribute security information.[26] A related initiative is to "[p]ursue deployment of intrusion prevention systems across the Federal enterprise." This step intends to improve situational awareness with more advanced capabilities to "identify and characterize malicious network traffic" in order to prevent its access to protected networks.[27]

Official US government statements also indicate the need to improve domain situational awareness. USCYBERCOM Commander Keith B. Alexander recently characterized the cyber domain as one with "strong adversary capabilities and weak situational awareness." He described intentions to:

> build an effective cyber-situational awareness in real time through a common, shareable operating picture. We must share indications in warning threat data at Net speed among and between the various operating domains. We must synchronize command-and-control of integrated defensive and offensive capabilities, also at Net speed. [28]

The CNCI also addresses the need for domain situational awareness capabilities. Specifically, one initiative is to "[c]onnect current cyber ops [operations] centers to enhance situational awareness." This element seeks to "support shared situational awareness and collaboration across six centers that are responsible for carrying out US cyber activities," through "shared analytic and collaborative technologies."[29] Similarly, DHS's Information Technology Sector-Specific Plan, an annex to the 2010 National Infrastructure Protection Plan, includes as a primary goal the need to enhance cyberspace situational awareness across the entire ICT sector.[30]

Capabilities

Progress towards these ends is evident, but legal and structural impediments remain. With respect to enterprise situational awareness, DHS Secretary Janet Napolitano recently announced that the Einstein 2 program, which can "automatically detect and disrupt malicious cyber activity," is almost fully deployed across the ".gov" domain. Development of the program's third iteration is already

underway.[31] For its part, DoD designated that one of USCYBERCOM's key missions is to elevate cyberspace situational awareness.[32] Additionally, according to Deputy Secretary of Defense William Lynn, DoD has deployed three layers of protection for US military networks, or the ".mil" domain,[33] of which two relate to industry best practices and appear to enhance situational awareness capabilities. These initiatives appear to have already stemmed malicious activity: security incidents on DoD networks decreased in 2010 for the first time in a decade.[34]

The US government has made other advancements at the domain level. In what probably constitutes the third and outermost layer of protection for its networks, DoD reportedly developed relationships with "tier 1" ISPs to identify and terminate malicious traffic from foreign sources before it reaches DoD networks.[35] DHS operates a "dashboard" that aggregates routing data and other information to provide real-time situational awareness about the state of the internet throughout the country. Critically, it can show when segments of the internet are down, which can help officials diagnose whether the root cause of the outage might be a natural disaster, a power outage, or perhaps an attack. The dashboard can even highlight areas with extreme network congestion, which could draw attention to infrastructure malfunctions.[36]

Recent government efforts reveal imperfect but strengthening capabilities. For example, a DHS-sponsored exercise series called "Cyber Storm" seeks to strengthen preparedness for a contingency in cyberspace, in part by improving enterprise and domain situational awareness. One of the exercise's four primary objectives is to "[v]alidate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information."[37] One of the key findings of the exercise's first iteration, held in February 2006, was that "[p]layers were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors."[38] The following exercise, held in March 2008, cites improvements but maintains that a better "[u]nderstanding [of] the interconnectedness and cause/effect relationships between actions taken by each organization would help to maintain broad situational awareness and galvanize a holistic approach to cyber response."[39]

Several factors, however, may impede the US government's prospects for improving cyberspace situational awareness.[40] First, with respect to laws, the executive branch operates on the basis of guidelines included in the Foreign Intelligence Surveillance Act, the Electronic Communications and Privacy Act, the PATRIOT Act (which includes provisions for National Security Letters), the Communications Assistance for Law Enforcement Act, and elsewhere. These laws can limit surveillance and other activities related to situational awareness, particularly with respect to data traversing US infrastructures or involving US persons.

Other checks, from a structural standpoint, include the market-driven and generally decentralized development of internet infrastructures. For example, US internet traffic destined abroad (and foreign traffic destined for the United States) may transit any of the approximately 19 undersea cable landing facilities along the US east and west coasts. Moreover, internet access in the United States is multimodal. That is, users may connect in a variety of ways, including by satellite. Finally, there are thousands of ISPs operating in the United States, of which perhaps a half dozen are considered "tier 1" providers. As a corollary, numerous US firms operate the international gateways that connect the internet in the United States to internet infrastructures in foreign countries. This multitude of infrastructure actors severely complicates efforts to establish comprehensive cyberspace domain situational awareness.

IV. Key features of the cyber domain in China[41]

In contrast to the abundance of US policy statements on cyberspace situational awareness, there are few indicators of Chinese views on the subject. In absolute terms, China's enterprise situational awareness status is probably less robust than its US counterparts. Software piracy—rampant in China—adversely affects software updates and patch implementation, management, and other essential aspects of system hygiene. Microsoft, for example, recently estimated that 90 percent of its software in use in China is pirated.[42] Depending on the vendor, unlicensed server software may not get critical patches and copies of antivirus software may not receive updated definitions. Pirated operating systems, web browsers, media players, and other software may also be affected. Notwithstanding recent efforts to counter the use of pirated software, it remains a common feature of even Chinese government computers.[43] Moreover, China consistently ranks in the top few countries with the most infected computers (although the United States is often in its company).[44]

Less is known about the state of China's domain situational awareness. However, an analysis of some of the key architectural features of the cyberspace domain in China can inform our understanding of China's cyber domain situational awareness prospects. Two features in particular—international gateways and filtering capabilities—bear closer examination.

International Gateways

The overwhelming majority of China's internet communications with the outside world transit just three international gateways located in Beijing in the north, Shanghai in the east, and Guangzhou in the south.[45] By design, this centralization of international internet connections allows Chinese authorities to exert a significant level of control over data traversing China's national-level networks.[46] As a result, according to an account by journalist James Fallows, Chinese authorities can:

> physically monitor all [internet] traffic into or out of the country. They do so by installing at each of these few "international gateways" a device called a "tapper" or "network sniffer," which can mirror every packet of data going in or out…. "Mirroring" is the term for normal copying or backup operations, and in this case real though extremely small mirrors are employed. Information travels along fiber-optic cables as little pulses of light, and as these travel through the Chinese gateway routers, numerous tiny mirrors bounce reflections of them to a separate set of… computers. [47]

Filtering Capabilities

This separate set of computers, known colloquially as China's "Great Firewall,"[48] allows Chinese authorities to surveil and filter internet traffic. The system leverages a set of mechanisms to evaluate and analyze data destined for networks outside China.[49] Most of this data is directed to the rest of the internet via undersea cables to transit points throughout East Asia. However, when the Great Firewall identifies data considered offensive by China's authorities, the system resets the attempted connection in order to terminate the data transmission.[50] Technical research corroborates Mr. Fallows' account that data transiting between internet destinations in China and abroad are indeed mirrored to "out of band" machines, which are separate and parallel to the core routers that facilitate the transactions.[51] Computer researchers refer to these machines as intrusion detection systems (IDS), defined by the National Institute of Standards and Technology (NIST) as applications or devices for "monitoring the events occurring in a computer system or network and

analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."[52]

China's IDS employs deep packet inspection (DPI), described by computer security firm Symantec as the ability "to look within the application payload of a packet or traffic stream and make decisions on the significance of that data based on the *content* of that data" (emphasis original).[53] This is opposed to less sophisticated utilities that only analyze data *labels*, such as packet headers, which contain important but less specific information like data origin and destination. In practice, for example, DPI allows the Great Firewall to not only determine when a user in China attempts to establish a connection to *www.bbc.co.uk* (label), but whether the specific page requested contains keywords related to the Falun Gong (content).

An important caveat here is that DPI technology is generally effective only on data sent "in the clear," or in unencrypted form. This weakness allows users to leverage virtual private networks (VPN) to "scale" the Great Firewall. Although Chinese authorities could simply block encrypted internet traffic destined abroad, such a move could immediately halt substantial levels of foreign business operations in China, which the government is loathe to do.[54] However, at least one firm with business activities in China[55] advertises DPI suites that use signatures to communicate a "broad range of criteria, header information, actual payload, bi-directional traffic information and the characteristics… even as applications get encrypted."[56] Such technologies raise questions about how long encrypted traffic can remain a sanctuary from China's data inspections.

V. Implications for situational awareness

There are at least five components of situational awareness: intelligence, surveillance, reconnaissance, environmental monitoring, and common operating picture. [57] For the purposes of this analysis, reconnaissance is how to find something; surveillance is how to track it; and intelligence is the actionable results of these (and related) efforts.[58] Environmental monitoring involves the attempt to understand natural and unnatural influences and events and their impact on a domain. Common operating picture is a holistic and shared view of information from numerous inputs and sources across a domain. Although complete treatment of how each concept applies to cyberspace is beyond the scope of this paper, all are at least somewhat affected by the architectural features of China's censorship regime.[59]

Intelligence: The Great Firewall's main function is traffic inspection and termination, but the system could conceivably employ features designed to collect intelligence. Although it would be infeasible to retain all of the mirrored internet traffic for any longer than it takes to conduct a cursory inspection, some data could be stored for later analysis and exploitation. If such a capability is in place, data could be flagged for retention at the router or IDS level based on predetermined parameters. Rules implemented within this system could direct potentially useful data to a storage device for further review by human analysts. [60] Though the existence of such an inspection regime is purely speculative, the possibility appears within reach of China's authorities. From a technical standpoint, it would even be less challenging than basic filtering (given that the central obstacle would be the review and manipulation of all data, which China currently does).

These potential intelligence-related features present more cause for concern when viewed in light of China's ability to essentially import internet traffic from abroad. Although by no means unique—ISPs in other nations have previously done the same thing—China briefly demonstrated this

capability in April 2010. In that incident—which could have been accidental—state-owned China Telecom propagated improper routing information that instructed US and other foreign internet traffic to transit Chinese servers. The event affected traffic to and from, among other things, the web domains associated with the Office of the Secretary of Defense and all four US military services. [61] Affected traffic would likely have transited the Great Firewall and thus could have been censored or exposed to any intelligence collection or analysis features inherent in the system.

Surveillance: China's control of the internet extends beyond censorship and into surveillance.[62] The general trend is well documented,[63] but specific architectural aspects of the Great Firewall enhance these capabilities. In particular, all information that transits the Great Firewall must include origin and destination information, such as Internet Protocol address or domain; these data could conceivably be logged according to rules triggered by keywords or other predetermined specifications.[64] Such information could have numerous applications; for example, it could explain accounts of software used by Chinese authorities that issues reports when specific users in China access banned websites.[65] Of note for people outside China, the Great Firewall reportedly has bidirectional functionality, meaning users outside China can be prevented from viewing content on sites hosted within China.[66] By extension, foreign users who attempt to connect to Chinese nodes may face some level of surveillance, to the extent that it is inherent in the systems that compose the Great Firewall.

Reconnaissance: If Chinese authorities leverage the Great Firewall to analyze traffic, the limited number of international gateways would simplify the process. That virtually all internet traffic between China and the outside world transits three locations would significantly bind the complexity of information mining.[67] Consider a scenario where Chinese authorities sought to locate a user based on a unique identifier, such as email address:[68] the fewer the transit points, the more efficient the search. For people and systems within China, it would be far more pragmatic to conduct reconnaissance activities at the ISP level, but the gateway level would serve to identify the correct ISP to approach in the event that that information was not already known to authorities. Again, bearing in mind the Great Firewall's bidirectional nature, such reconnaissance activities may also have implications for users outside China communicating with users or connecting to sites inside China. China's network infrastructure abroad may also have a suite of features that, though perhaps harmless, could facilitate reconnaissance. China Telecom Americas Corporation's promotional materials call its network "traceable," with "real-time monitoring and reporting."[69]

Environmental Monitoring: One of the unique features of the cyberspace domain is the relative indivisibility of the domain itself from a given system within that domain. In the space domain, the evaluation of space weather and events to determine how they might affect space systems, such as satellites, is fairly straightforward (though certainly not simple). In cyberspace, enterprises should similarly seek to understand significant "environmental" events, such as viruses and malfunctions in exterior networks.[70] But in the sense that the government has a vital interest in ensuring that the cyber domain itself—and all domestic segments in particular—remain operational, it would be arbitrary to separate a system of interest from other networks and infrastructures. For example, a key government entity might perfectly defend its networks, but if an attack disrupts upstream systems—such as the entity's ISP—key systems could still be denied access to the internet. In this light, environmental monitoring should include any substantial event in the cyber domain.

Some evidence suggests that Chinese authorities previously configured routers on national-level networks to filter virus-related traffic.[71] To bolster this capability, gateway filtering could operate in a similar capacity. The limited number of gateways creates comprehensive vantage points that could

help inform battle damage assessment across networks and enable mitigation efforts, particularly if an attack lacks a readily identifiable signature to block. For example, monitoring bandwidth might help administrators estimate the effects of distributed denial of service (DDoS) attacks targeting numerous sites across multiple ISPs. Other "sensors" at the gateways could monitor routing data to provide reports on route hijacking or other unusual events.

Common Operating Picture: The confluence of all traffic at just three international gateways could also help enable threat characterization analysis. China has an active marketplace for data mining utilities, frequently used for surveillance applications,[72] which may offer efficient ways to identify and parse events and trends on the internet. Unity of effort is another imperative related to common operating picture, and these "hubs" could facilitate a coordinated response by various Chinese entities in the event of a cyberattack or counterattack. Moreover, any of the monitoring scenarios described above could have implications for tracking "red" and "blue" forces (in China's usage, friendly and adversary, respectively), which is a key component of traditional common operating picture requirements.

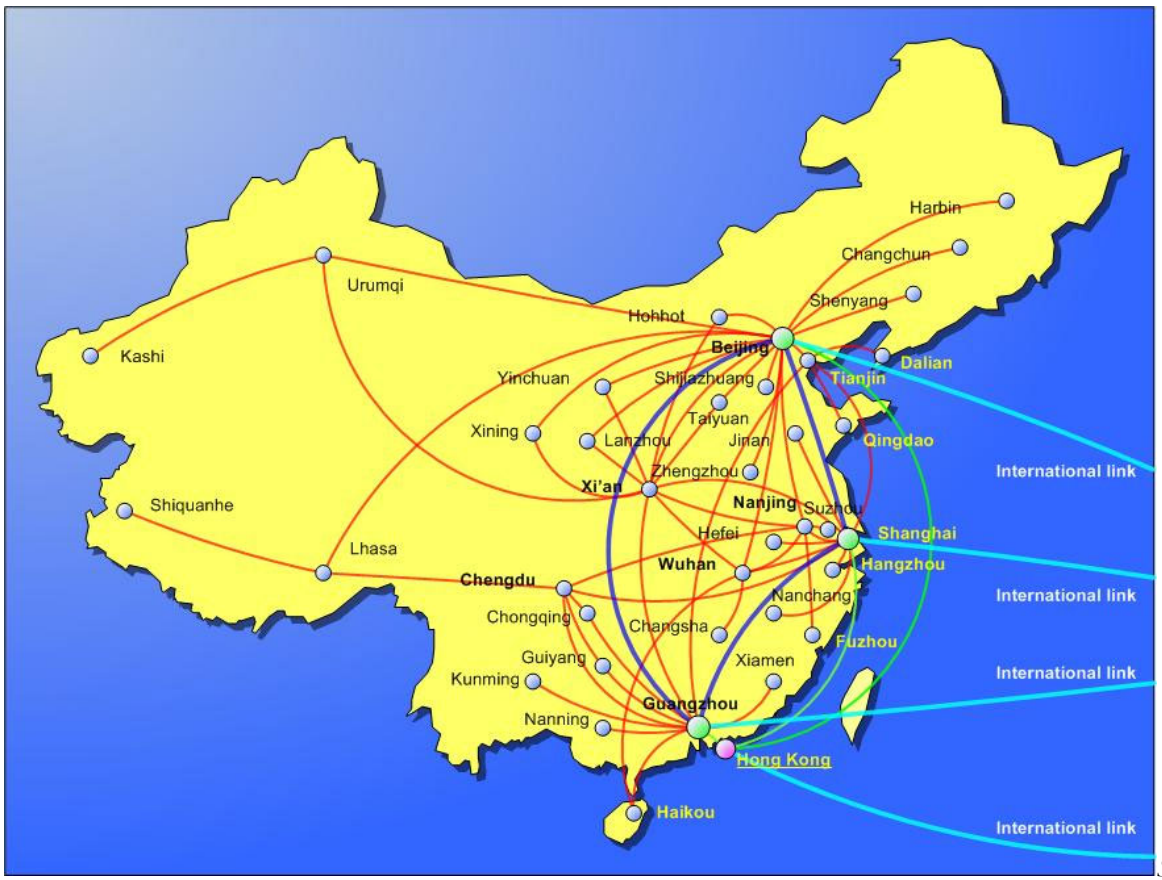
VI. Balancing equities

Although situational awareness is clearly a desirable end in the cyber domain, the means employed by China imply some important tradeoffs. Three in particular merit consideration. First, states must determine how to allocate resources in the cyber domain, and skilled personnel might well be the key constraint. Second, states may have an interest in the topology of their networks, particularly the extent to which infrastructure should be centralized. Third, if states view cyberspace as a potential domain of conflict, infrastructure and force structure should be optimized to address contingencies based on threat assessments.

Resource allocation: China's censorship system is rooted in the Chinese Communist Party's (CCP) perception about how best to maintain regime stability. Thus, from a defense planning perspective, derivative gains in situational awareness are essentially free. However, it is unclear that Chinese investments in ICT architecture reflect risk analyses that weigh censorship against the potential implications of a cyberwar, which could also affect the CCP's ability to maintain social control. Assuming a finite pool of human capital with the advanced skills required to operate in the cyber domain, man-hours expended on censorship activities—even with their ancillary benefits for cyberspace situational awareness—come at the expense of other cyberwar-related capabilities.[73] These could include, among other things, cyber defense, cyber offense, command and control in cyberspace, and cyberspace reconstitution capabilities.

Network topology: The CCP's perceived need for censorship influenced the development of China's internet architecture, resulting in considerable centralization. Though helpful for filtering and situational awareness, this comes at the expense of robust redundancy. This may be an acceptable trade-off at the enterprise level.[74] However, centralized architecture at the domain level raises questions about the sustainability of internet access in a conflict scenario. This could have implications for China's ability to retaliate in cyberspace, which raises two key concerns. First, the absence of an assured second strike capability in cyberspace could give China a destabilizing incentive to strike preemptively.[75] Second, denied access to the cyber domain could promote escalation into other domains of war.[76]

Figure 1: China's primary international internet connections[77]



Source: China Telecom, USA

China's international gateways connect its six national-level networks[78] to one or more of seven international land-submarine cables that link China to the rest of the internet.[79] Causing a power outage in the three cities that host international gateway facilities, a conceivable objective in the context of conflict in cyberspace, could substantially isolate China from the rest of the internet.[80] The physical disruption of one or more of the China's international submarine cables could cause even greater damage. Attacks on such cables would be a severe measure, as their disruption would adversely affect the internet throughout the region.[81] Moreover, US cyberspace operations have been canceled in the past for fear of unknown or uncontrollable effects.[82] Still, while global telecommunications interdependence may be more entrenched today than ever before, the precedent for targeting undersea communications cables dates back to the First World War.[83] Such assets could be targeted again in a serious contingency.

Domain optimization: The discussion above suggests that China's domain configuration yields some benefits for cyberspace situational awareness at the expense of other features. Although China's internet architecture probably evolved independently of these considerations, the Chinese government is nonetheless left with forces and infrastructure that appear better equipped to handle limited rather than total conflicts in cyberspace. For example, in a constrained engagement, situational awareness might be the primary consideration, as it could enable smart defense and mitigation techniques. By contrast, in a more intense scenario, emphasis might shift to favor

offensive actions. To the extent that resources available for each mission are drawn from the same pool, this would relatively diminish the importance assigned to domain situational awareness activities. Of course, it remains unknown whether this orientation aligns with the Chinese government's threat perception regarding the relative likelihood of limited versus severe conflict in cyberspace.

VII. Policy Implications

The United States must consider the security implications of internet filtering activities. This may influence the urgency and means with which US policy seeks to address internet censorship and related activities abroad. By extension, a policy that accounts for the nexus between certain censorship activities and cyberspace situational awareness could alter present views about the permissibility of US firms' assistance to foreign countries' censorship activities.[84] In particular, situations that involve technology transfer could require some sort of regulation or oversight.[85]

The United States must also "balance equities" in cyberspace. One of the defining characteristics of the United States' approach to the cyber domain, particularly when compared to China, is the numerous limitations on the US government's ability to collect information that might aid situational awareness. While the United States requires improved cyberspace situational awareness, it remains unclear whether this end necessitates or justifies drastic adjustments to legal and structural checks. Alternative technologies or systems—perhaps even administered by private entities, such as a consortium of ISPs—might yield sufficient domain-level situational awareness capabilities. Such a mechanism might eventually serve as the foundation for a wider application of what appears to be DoD's approach to stopping malicious traffic at the "tier 1" ISP level.[86] Policymakers must recognize, however, that such activities are not costless and could require government support through subsidies, tax breaks, or other incentives.

In the event that improvements do require alterations to existing legal and structural checks, each change should reflect a deliberate, inclusive, and transparent review process. Moreover, each potential change ought to be justified through cost-benefit analyses related to resource allocation, network topology, and domain optimization, as described above, or another compelling rationale. Finally, on a tactical level, internet architecture should be a central factor in the context of defensive and offensive cyberspace operational planning.

About the Author

Robert Sheldon is a Policy Analyst for Military and Security Affairs at the US-China Economic and Security Review Commission. He previously worked on various cyber issues in law enforcement, intelligence, and defense-related capacities. Sheldon has an MA in Security Policy Studies and a BS in Computer and Digital Forensics. He can be reached at x@longtelegrams.com.

Notes

[1] U.S. Congress. Senate. Senate Armed Services. By Keith B. Alexander. 112th Cong. S. Doc. March 15, 2010. http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

[2] Lynn III, William F. "Defending a New Domain." *Foreign Affairs* 89, no. 5 (September/October 2010): 98.

[3] U.S. Department of Defense. "Joint Statement by Secretary Gates and Secretary Napolitano on Enhancing Coordination to Secure America's Cyber Networks." News release, October 13, 2010. http://www.defense.gov/releases/release.aspx?releaseid=13965. Full text of the agreement available at http://www.defense.gov/news/d20101013moa.pdf.

[4] Corrin, Amber. "DISA Creates 'demilitarized Zone' for Unclassified Network." *Federal Computer Week*, January 7, 2011. http://fcw.com/Articles/2011/01/07/DISA-panel-DOD-DMZ.aspx.

[5] For example, Mearsheimer, John J. "China's Unpeaceful Rise." *Current History* 105, no. 690 (April 2006): 160-62. http://mearsheimer.uchicago.edu/pdfs/A0051.pdf.

[6] For example, Lopez, C. Todd. "Next War Will Begin in Cyberspace, Experts Predict." *Army News Service*, February 27, 2009. http://www.army.mil/-news/2009/02/27/17561-next-war-will-begin-in-cyberspace-experts-predict/.

[7] For example, U.S.-China Economic and Security Review Commission. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* By Bryan A. Krekel. McLean, VA: Northrop Grumman, Information Systems Sector, 2009. pp. 10-29. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

[8] "China." OpenNet Initiative. June 15, 2009. Accessed January 30, 2011. http://opennet.net/research/profiles/china.

[9] The case about implications for human rights is best articulated in Clinton, Hillary R. "Remarks on Internet Freedom." Speech, Newseum, Washington, DC, January 21, 2010. http://www.state.gov/secretary/rm/2010/01/135519.htm. To its credit, this speech identifies one important security implication: "asymmetrical access to information is one of the leading causes of interstate conflict."

[10] For example, Google. *Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information.* Report. Accessed January 22, 2011. http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/trade_free_flow_of_information.pdf.

[11] This article discusses cyberspace situational awareness primarily as it relates to potential cyber conflict between the U.S. and China. This article does not take a position on the likelihood of such a scenario. For a nuanced take on how China might seek to employ offensive cyber attacks in a contingency against the U.S., see Libicki, Martin C. "Chinese Use of Cybewar as an Antiaccess Strategy: Two scenarios." Testimony to the U.S.-China Economic and Security Review Commission, January 27, 2011. http://www.uscc.gov/hearings/2011hearings/written_testimonies/11_01_27_wrt/11_1_27_libicki_testimony.pdf. Of course, general cyberspace situational awareness capabilities would also be of value for combating cyberterrorism, an arguably more likely contingency.

[12] This paper does not include specific policy recommendations, a discussion about the desirability of "cyberwar" as a tool of statecraft, or meaningful treatment of privacy issues or the human rights implications of either censorship or conflict in cyberspace. Each merits due consideration, but are outside the scope of this analysis.

[13] Lessig, Lawrence. *Code and Other Laws of Cyberspace.* New York: Basic Books, 1999.

[14] U.S. Joint Chiefs Staff. Office of the Chairman. *The National Military Strategy for Cyberspace Operations.* Washington, DC: Department of Defense, 2006. p. 5. http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf.

[15] "About Filtering." OpenNet Initiative. Accessed January 30, 2011. http://opennet.net/about-filtering/. This analysis substitutes the term "organizations" for the original "institutions" to avoid conflation with the traditional social science definition of the latter. I am indebted to an anonymous reviewer for identifying the potential for confusion.

[16] Deibert, Ronald, John G. Palfrey, and Jonathan Zittrain. *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010. p 465. The Green Dam Youth Escort affair was a less successful example. See Wines, Michael. "China Scales Back Software Filter Plan." *New York Times*, August 13, 2009. http://www.nytimes.com/2009/08/14/world/asia/14censor.html. However, Green Dam's persistence at Internet cafes, schools, and libraries highlights China's successes at the organizational level of control.

[17] In 2010, following revelations about the Aurora exploitations, Chinese authorities used a license renewal application as a lever to force Google to stop automatically redirecting mainland Chinese users to its uncensored Hong Kong site. See Lee, Melanie, and Emma Graham-Harrison. "UPDATE 4-Google Tweaks China Site in Bid to Keep License." *Reuters*, June 29, 2010. http://www.reuters.com/article/idUSN2914697820100629.

[18] For example, MacKinnon, Rebecca. "Chinese Blogger Takes China Telecom to Court for Censorship." *RConversation* (web log), August 6, 2007. http://rconversation.blogs.com/rconversation/2007/08/chinese-blogger.html.

[19] This article focuses specifically on architecture because of its relatively static nature. Control at other levels could be intensified or moderated on a more rapid basis.

[20] Specifically, the term does not appear in *JP1-02 DOD Dictionary of Military and Associated Terms (as Amended through September 2010)*.

[21] For example, U.S. Department of Homeland Security. *Fact Sheet: Protecting America's Critical Infrastructure – Cyber Security*. February 15, 2005. http://www.dhs.gov/xnews/releases/press_release_0620.shtm. Of note, the term does not appear in U.S. Executive Office of the President. *National Strategy to Secure Cyberspace*. February 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

[22] U.S. Joint Chiefs of Staff, 2006. p. 17.

[23] This distinction draws from one made for risk management approaches in U.S. Department of Homeland Security. *Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. 2010. p. 2. http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech-2010.pdf.

[24] Mulvenon, James. "CCSA Study One IPR." Cyber Conflict Studies Association. September 2010. Slide 4. https://sites.google.com/a/cyberconflict.org/study-1/home/study-1-documents/study-1-presentation.

[25] U.S. Chief Information Officer Council. *FY 2011 President's Budget, Analytical Perspectives, Special Topics, Chapter 19, Information Technology*. Accessed January 16, 2011. p. 4. http://www.cio.gov/pages.cfm/page/Chapter-19-Information-Technology-Page-4.

[26] U.S. Executive Office of the President. *Comprehensive National Cybersecurity Initiative*. Accessed January 30, 2011. p. 2. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf. Intrusion detection systems are described in more detail below.

[27] Executive Office of the President. *Comprehensive National Cybersecurity Initiative*. p. 3.

[28] Alexander, Keith. "Cybersecurity Discussion with General Keith B. Alexander, Director of the NSA, Commander of U.S. Cyber Command." Speech, Center for Strategic and International Studies, Washington, DC, June 2, 2010. http://csis.org/event/cybersecurity-discussion-general-keith-b-alexander-director-national-security-agency.

[29] U.S. Executive Office of the President. *Comprehensive National Cybersecurity Initiative*. pp. 3-4.

[30] See in particular goals two and four. U.S. Department of Homeland Security. *Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. p. 2.

[31] Miller, Jason. "DHS Readies New Tools to Combat Cyber Attacks." *Federal News Radio*, January 28, 2011. http://www.federalnewsradio.com/?nid=35&sid=225164.

[32] U.S. Congress. Senate. 2010. p. 1; and Rosenzweig, Paul. "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence." In *Proceedings of a Workshop on Deterring Cyberattacks Informing Strategies and Developing Options for U.S. Policy*, edited by National Research Council, p. 252. Washington, DC: National Academies Press, 2010.

[33] Lynn III, William F. "Defending a New Domain." pp. 103-4.

[34] U.S.-China Economic and Security Review Commission. *2010 Annual Report to Congress*. Washington, DC: Government Printing Office, 2010. pp. 236-7. www.uscc.gov/annual_report/2010/annual_report_full_10.pdf.

[35] Specifically, "DOD, working with DHS, has begun an approach currently named 'Active Defense' that can be described as working with tier 1 service providers to intercept malware from foreign sources." Representative Langevin, James R., Michael T. McCaul, Scott Charney, and Lt. General Harry Raduege,

USAF (ret.). "Cybersecurity Two Years Later." Center for Strategic and International Studies. January 2010. p. 10. http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

[36] Contractor to the U.S. Department of Homeland Security. E-mail message to author. January 2011.

[37] U.S. Department of Homeland Security. *Cyber Storm: Securing Cyber Space*. Accessed January 22, 2011. http://www.dhs.gov/files/training/gc_1204738275985.shtm.

[38] U.S. Department of Homeland Security. National Cyber Security Division. *Cyber Storm Exercise Report*. September 12, 2006. http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf.

[39] U.S. Department of Homeland Security. National Cyber Security Division, Office of Cybersecurity and Communications. *Cyber Storm II Final Report*. July 2009. http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf. Findings from Cyber Storm III (September 2010) had not been released at the time of this writing.

[40] Most fundamentally, situational awareness-enabling technologies lag behind threats (in other words, "necessity is the mother of invention"). This lag is consistent with other weapons technologies: intercontinental ballistic missiles, for example, came before the early warning satellites used to detect launches. However, this dynamic also affects China (and all other actors in cyberspace), and will therefore not be treated here.

[41] This analysis excludes Hong Kong and Macau Special Administrative Regions, which have fairly open ICT environments.

[42] Brodkin, Jon. "Ballmer to Hu: 90% of Microsoft Customers in China Using Pirated Software." *Network World*, January 21, 2011. http://www.networkworld.com/news/2011/012111-ballmer-hu-china-software-piracy.html. Note, however, that Microsoft makes security updates available to unlicensed users. See Cooke, Paul. "Who Gets Windows Security Updates?" *Windows Security Blog* (web log), April 27, 2009. http://windowsteamblog.com/windows/b/windowssecurity/archive/2009/04/27/who-gets-windows-security-updates.aspx.

[43] Wines, Michael. "China to Begin Crackdown on Pirated Software in 2011." *New York Times*, January 7, 2011. http://www.nytimes.com/2011/01/08/business/global/08piracy.html?src=busln.

[44] The author has not established causation between software piracy and compromised machines, although the variables may correlate. For one report about the volume of China's infected machines, see Nakashima, Ellen. "China leads the world in hacked computers, McAfee study says." Washington Post, February 15, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/14/AR2010021403817.html. *Caveat lector*: these figures probably do not represent a scientific sample. Moreover, the data appears to be in absolute terms, whereas infections as a percentage of total online systems may be a more instructive measure for the purposes of this analysis.

[45] There are several important qualifiers. China Telecom operates terrestrial cables to Vietnam, Laos, Myanmar, India, Kazakhstan, Russia, and Europe (via Russia). With the exception of the latter, these cables carry marginal levels of traffic (for example, the China-India cable's capacity is 44.21mb/s, or about 0.22 percent of the firm's capacity to Japan), and likely employ some variation of the same gateway-level filtering mechanisms described below. China Telecom Americas. "International Internet Bandwidth." Undated. Accessed February 19, 2011. http://www.chinatelecomusa.com/content.asp?pl=627&sl=637&contentid=727&id=1&indexid=0. Similarly, China Unicom, which also has a stake in the notable China-Europe cables, operates low bandwidth terrestrial cables to Vietnam, Myanmar, Kazakhstan, Russia, Mongolia, and North Korea. China Unicom. "Global Networks." Undated. Accessed February 19, 2011. http://eng.chinaunicom.com/partner/Eng_ywhz/GlobalN/index.html. Finally, satellites, a once robust mode of Internet access in China, now carry little or no Internet traffic, according to recent routing data and traceroute measurements. Contractor to the U.S. Department of Homeland Security. E-mail message to author. January 2011.

[46] Cherry, Steven. "The Net Effect." *IEEE Spectrum*, June 2005. Accessed January 6, 2011. http://spectrum.ieee.org/computing/networks/the-net-effect/0.

[47] Fallows. "The Connection Has Been Reset." 2008.

[48] Consistent with popular usage, this paper uses the term "Great Firewall" in place of the proper term, "Golden Shield." For information about the latter, see Walton, Greg. International Centre for Human Rights and Democratic Development. *China's Golden Shield*. Report. 2001. pp. 14-7. http://www.dd-rd.ca/site/lPDF/publications/globalization/CGSlENG.PDF.

[49] For a general explanation of these mechanisms, see Fallows, "The Connection Has Been Reset." 2008. For a technical explanation, see Clayton, Richard, Steven J. Murdoch, and Robert N. M. Watson. "Ignoring the Great Firewall of China." Proceedings of 6th Workshop on Privacy Enhancing Technologies (June 2006), Cambridge. http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; and Lowe, Graham, Patrick Winters, and Michael L. Marcus. "The Great

DNS Wall of China." MS, New York University. Accessed December 21, 2007. http://cs.nyu.edu/~pcw216/work/nds/final.pdf.

[50] Deibert, Ronald, John G. Palfrey, and Jonathan Zittrain. *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010. p 467.

[51] Clayton, Murdoch, and Watson. "Ignoring the Great Firewall of China," 2006. Section 4. However, there is also reason to believe that some blocking occurs at the router level, thus obviating the need to pass data to an IDS. Villeneuve, Nart. "Censorship Is in the Router." *Nartv* (web log), June 3, 2005. http://www.nartv.org/2005/06/03/censorship-is-in-the-router/.

[52] U.S. Department of Commerce. National Institute of Standards and Technology. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. By Karen Scarfone and Peter Mell. 800-94. Gaithersburg, MD: NIST, 2007.p. ES-1. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[53] Dubrawsky, Ido. "Firewall Evolution - Deep Packet Inspection." Symantec. July 28, 2003. http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection. However, there is some confusion about whether China's DPI efforts occur at the ISP level or at international gateways, or both. Rhodes, Christopher, and Loretta Chao. "Iran's Web Spying Aided By Western Technology." *Wall Street Journal*, June 22, 2009. http://online.wsj.com/article/SB124562668777335653.html#ixzz1B8fecNwz.

[54] Fallows. "The Connection Has Been Reset." 2008.

[55] Procea Networks. "Procera Networks Gains Momentum in Asia." News release. Accessed January 16, 2011. http://www.proceranetworks.com/recent-press-releases-archive/388-procera-networks-gains-momentum-in-asia.html; and "Contact Us." Procera Networks. Accessed January 18, 2011. http://www.proceranetworks.com/partners/partners-overview.html.

[56] "About." Procera Networks. Accessed January 31, 2011. http://china.proceranetworks.com/about-procera.html.

[57] Adapted from U.S. Joint Chiefs of Staff. *Space Operations*. Washington, D.C., 2009. Accessed January 20, 2011. http://www.fas.org/irp/doddir/dod/jp3_14.pdf. Chapter II-7-8. The official definition for each, albeit for the purposes of space, are contained within. There is precedent for the use of existing air and space doctrine to inform discussion about cyberspace doctrine, which is comparatively underdeveloped. See, for example, Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009. p. 163 at note 3.

[58] This is adapted from a pithy formulation by then-secretary of defense Donald Rumsfeld. See Deptula, David A., and R. Greg Brown. "A House Divided: The Indivisibility of Intelligence, Surveillance, and Reconnaissance." *Air & Space Power Journal*, June 1, 2008. http://www.airpower.au.af.mil/airchronicles/apj/apj08/sum08/deptula.html.

[59] For this section, the author has attempted not to overstate the potential significance of international gateways. Readers should bear in mind, however, that the hypotheticals described here (subject to included qualifications) could probably occur at the ISP level, albeit in a more fragmented and thus less effectual fashion.

[60] Wortzel, Larry, and Rodney Joffe. "China Internet 'Hijacking': Your Questions Answered." *PBS Newshour*, December 2, 2010. http://www.pbs.org/newshour/updates/science/july-dec10/chinainternet_12-02.html#q9.

[61] U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress*. pp. 241-4. For some fair counterpoints to this account, see Cowie, James. "China's 18-Minute Mystery." Renesys Blog (web log), November 18, 2010. http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml.

[62] Villeneuve, Nart. "Human Rights and Malware Attacks." In *"China's Internet": Staking Digital Ground*. Vol. CRF 2010. Series 2. 2010. http://www.hrichina.org/public/contents/article?revision_id=175306&item_id=175263.

[63] See, for example, Villeneuve, Nart. *BREACHING TRUST: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform*. Report no. JR01-2008. October 1, 2008. p. 4. http://www.infowar-monitor.net/breachingtrust/; and Information Warfare Monitor. *Tracking GhostNet: Investigating a Cyber Espionage Network*. Report no. JR02-2009. March 29, 2009. p. 28. http://www.tracking-ghost.net. These examples were enabled by means other than the architectural aspects of the Great Firewall.

[64] China's ISPs and ICPs have data retention obligations. Deibert, Palfrey, Rohozinski, and Zittrain. *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. 2010. p. 465.

[65] Brady, Anne-Marie. *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*. Plymouth UK: Rowman & Littlefield, 2008. p. 132.

[66] Fallows. "The Connection Has Been Reset." 2008. http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/.

[67] Deibert, Palfrey, Rohozinski, and Zittrain. *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. 2010. p. 469.

[68] For example, Brady. *Marketing Dictatorship*. 2008. p. 132; and *Reuters*. "Chinese Internet censors blamed for email chaos." July 18, 2007. http://www.reuters.com/article/2007/07/18/us-china-internet-idUSPEK9185520070718. The latter report describes email filtering that affected users outside China.
[69] China Telecom Americas Corporation. "Next Generation Carrying Network CN2." 2010. p. 2. http://www.chinatelecomusa.com/files/CN2_Americas.pdf.
[70] The figurative use of the term "environmental" events here is not to suggest that literal environmental events should not receive due consideration. For example, Rauscher, Karl Frederuck. *ROGUCCI: the Report*. Report. IEEE Communications Society, 2010. p. 154-66. http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf; and "History." Space Weather Canada. Accessed January 22, 2011. http://www.spaceweather.gc.ca/se-chr1-eng.php.
[71] This example relates to the 2001 "Code Red" worm. Villeneuve. "Censorship Is In the Router." 2005.
[72] Deibert, Palfrey, Rohozinski, and Zittrain. *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. 2010. P. 464.
[73] Granted, in a country with over 1.3 billion citizens, the labor pool is probably quite robust. Still, as more and more of those citizens gain access to communications technologies, and as those technologies become more data-intensive, evermore people will probably be required to maintain the censorship regime. Also, although this does not necessarily indicate a labor shortage in the Chinese government, China's military has for years appropriated civilians, in the form of Information Warfare Militias, for use in potential cyberwar scenarios. U.S.-China Economic and Security Review Commission. *2009 Annual Report to Congress*. Washington, DC: Government Printing Office, 2009. pp. 173-4. http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf.
[74] The U.S. Government appears to value situational awareness over redundancy at the enterprise level. Consider the Trusted Internet Connection (TIC) Initiative, billed as a way to enhance situational awareness by reducing from over 1,000 to about 50 the number of connections between federal government networks and the Internet. See Miller, Jason. "OMB Directs Agencies to Close off Most Internet Links." *Federal Computer Week*, December 2, 2007. http://fcw.com/Articles/2007/12/02/OMB-directs-agencies-to-close-off-most-Internet-links.aspx. The goal of 50 was later upwardly revised. Lais, Sami. "TIC Initiative Gathers Speed." *Federal Computer Week*, September 23, 2009. http://fcw.com/articles/2009/09/22/kundra-tic-deadlines.aspx.
[75] This assumes that an effectual second strike would need to be launched domestically, which may not be the case. China could well have capabilities "forward deployed." In particular, Hong Kong (again, not treated in this analysis) is a regional Internet hub that probably could not be forcibly isolated from the Internet without catastrophic spill-over effects throughout Asia and the Pacific. Forces could also be deployed to foreign countries. For example, authoritative Chinese military writings call for cyber attacks against the United States to be launched from within the United States. Mulvenon, James. "Information Warfare and China's Cyber-warfare Capabilities." Speech, Carnegie Endowment for International Peace, Washington, D.C. February 10, 2011.
[76] For an accessible discussion of vertical escalation, see Morgan, Forrest E., Karl P. Meuller, and Evan S. Medieros. *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA: RAND, 2008. p. 18. http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf.
[77] This figure, which is undated, does not include the international terrestrial cables referenced above.
[78] PRC. China Internet Network Information Center. *26th Statistical Report on Internet Development in China*. July 2010. p. 24. http://www.cnnic.cn/uploadfiles/pdf/2010/8/24/93145.pdf.
[79] PRC. State Council. Information Office. *The Internet in China*. June 8, 2010. Section I. http://www.china.org.cn/government/whitepaper/2010-06/08/content_20208003.htm.
[80] The same may apply for the coastal cities that host the cable landing facilities: Qingdao in the north, Chongming and Nanhua in the east, and Shantao in the south.
[81] Rauscher. "ROGUCCI: the report." 2010. pp. 154-66.
[82] Markoff, John, and Thom Shanker. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *New York Times*, August 1, 2009. http://www.nytimes.com/2009/08/02/us/politics/02cyber.html; and Smith, Charles R. "Cyber War Against Iraq." *Newsmax*, March 13, 2003. http://archive.newsmax.com/archives/articles/2003/3/12/134712.shtml.
[83] Murphy, Dennis M. Review of *Nexus: Strategic Communications and American Security in World War I*. *Parameters*, Winter 2008-2009. p. 147.
[84] This is an exceedingly delicate matter. Different countries (even throughout the West) have different standards of free speech, and U.S. firms operating abroad ought to have some degree of latitude to comply with local laws and regulations.
[85] Best practices developed—and strictly adhered to—by industry itself could obviate the need for governmental regulation.

[86] Any such activities must offer sufficient protections to both users (especially with respect to expression) and ISPs and other operators (especially with respect to liability). "Threading the needle" on this issue socio-politically will be well more challenging than the technical requirements.

The Dollar's Vulnerability and the Threat to National Security

MAJ Neil C. Everingham, US Army, and Professor David A. Anderson, USMC (ret)

Introduction

The decline of the United States as a great power has been a popular topic with pundits for years. The same is true of the United States dollar (subsequently referred to as "dollar") and its role as the world's dominant international currency. Not surprisingly, the loss of such currency status has historically coincided with the loss of great power status.[1] These two interrelated issues have recently become of increasing concern due to rising levels of United States deficit spending and a growing debt burden. The unease revolves around whether the dollar's status, and by extension, the United States' international leadership role, are still viable as its debt approaches record levels in absolute terms. Epitomizing this concern are the recent calls for an alternative to the dollar as the world's central international currency by China, Russia, Brazil, and some OPEC nations, coupled with increasing pressure from large vote-carrying members of the International Monetary Fund (IMF) for the United States to reduce its voting shares.

The purpose of this study is to identify looming vulnerabilities that may lead to the demise of the dollar undermining United States power and compromising its national security. In identifying vulnerabilities, we consider economists' views of international currency dominance and Benjamin J. Cohen's state of power theory, apply those views to the historical case of the United Kingdom, and then compare that to the present-day US in light of the National Security Strategy.

Modeling for Analysis

There are two opposing thoughts on the potential decline of the United States' international leadership that help shape this examination. Paul Kennedy, of Yale University, wrote in 1987 that the transition between great powers was a slow process that centered on the incumbent's struggle to balance short-term national security demands and long-term economic interests.[2] The inability to do so can lead to high levels of debt undermining overall economic viability. Niall Ferguson, of Harvard University, disagrees with Kennedy's model of a gradual rise and fall. Instead, he suggests great powers are complex adaptive systems that collapse as the result of sudden and catastrophic malfunctions, caused by their inability to finance public debt that accumulates due to high levels of deficit spending.[3] The United States has avoided this problem, in part, because of the dollar's international role.

---

[1] Jeffrey A. Frankel, "Still the Lingua Franka: The Exaggerated Death of the Dollar" *Foreign Affairs* 74, no. 4 (July 1995), 12.

[2] Paul Kennedy, *The Rise and Fall of the Great Powers* (New York: Vintage Books, 1989), 536, 540.

[3] Niall Ferguson, "Complexity and Collapse: Empires on the Edge of Chaos," *Foreign Affairs* 89, no. 2 (March/ April 2010): 20, 30.

The central purpose of an international currency today is to serve "as a store of value for central banks' and governments' international reserves."[4] While this may be the central role of today's international currencies, there are two other functions: to serve as units of account denominating international obligations and pricing commodities, and as media of exchange for transactions between other currencies.[5] The dollar is currently the primary international currency fulfilling each of these roles, which provide financial and security benefits to the US. Two principle benefits of the dollar's special status as the leading international currency are a regular inflow of foreign financing that keeps the United States interest payments on its debt low and its current and capital accounts in balance, thus enabling relatively large and sustainable deficit spending.[6]

Based on the theory of international currencies, a nation must have a relatively large economy for its currency to ascend to an international role. Once elevated, it becomes a competitor for the predominant role in international finance, which it will only achieve if it is dominant in trade. Therefore, it must have the dominant share of world trade volume and should lead in the value of its exports. Helen Rey of the London Business School finds that trade flows are the key determinant in currency internationalization.[7] Paul Krugman finds that only the currency of a nation that is important in world payments can serve as an international vehicle currency and that once that role is established it is self-reinforcing.[8] The payments are the result of imports and exports; thus, to be important in world trade a nation must be active in trade, which reinforces Rey's findings. The process is reinforcing because once the role of vehicle currency is established, the transactions in that currency swell due to decreasing transaction costs. Krugman also finds that the process of change between vehicle currencies is catastrophic, as an amplifying loop of declining trade leads to increasing transaction costs and further declines in trade volume.[9]

Based on the ideal economic structure, the nation of the lead international currency should also be a net creditor and possess a current account surplus. Once this structure has been achieved, the nation enjoys financial benefits as well as increased power in the international state system. Having gained this predominant position, the importance of the currency in trade reinforces the currency's strength. The nation risks losing its position as an international currency by running up a gross government debt that results in a debt to GDP ratio of over 90% which correlates with increased inflation and low real economic growth. [10] [11] This erodes confidence in the currency as a store of

---

[4] Barry Eichengreen, "Sterling's Past, Dollar's Future: Historical Perspectives on Reserve Currency Competition" (Lecture, Economic History Society, Leicester, UK, April 10, 2005), 2.

[5] Paul Krugman, "Vehicle Currencies and the Structure of International Exchange," *Journal of Money, Credit, and Banking*, 12, no. 3, (August 1980): 513.

[6] Congressional Research Service, *Dollar Crisis: Prospects and Implications,* by Craig K. Elwell, RL34311 (Washington, DC: Government Printing Office, January 8, 2008), 6.

[7] Rey, Helene. "International Trade and Currency Exchange." *The Review of Economic Studies 68, no. 2*, (April 2001): 457.

[8] Krugman, "Vehicle Currencies and the Structure of International Exchange," 523.

[9] Ibid.

[10] Carmen M. Reinhart and Kenneth S Rogoff, "Growth in a Time of Debt," National Bureau of Economic Research working paper15639, Cambridge, MA (January 2010): 9.

[11] Reinhart and Rogoff, find a positive correlation between rising inflation and a high gross government debt to GDP ratio, defined as higher than 90% in the United States. Therefore, the ratio of gross government debt to GDP should be a key factor in evaluating the fit of an international currency for a leading reserve role.

value and fits with the logic that a nation should only resort to expansionary fiscal policy in times of desperation.

Finally, Benjamin J. Cohen's state of power theory has noteworthy application. Cohen identifies two operational dimensions of state power: the ability to control the behavior of others and the ability to act unilaterally.[12] These dimensions operate within a framework of two kinds of state power in a political economy, relational and structural—relational being the ability to get another power to do something they would not normally do, while structural power is the ability to shape the framework of international relations.[13] Clearly, both types of power are important, but structural power, by allowing a nation greater influence in creating future systems, is the more beneficial. Cohen finds that the store of value role of an international currency increases the issuing nation's autonomy, thus increasing its relational power.[14] The more significant structural power derives from a currency's international dominance of all three roles of money:

1. as a store of value for central banks' and governments' international reserves
2. as a unit of accounting denominating international obligations and pricing commodities
3. as a unit of exchange for transactions between other currencies[15] [16]

Thus, all nations whose currency serves as an international reserve enjoy a proportional increase in international autonomy and influence. However, the nation whose currency dominates all three roles has the advantage of shaping the rules of international relations. It follows that the dollar's central place in all three roles contributes to the foundation of United States international power. Therefore, preserving the dollar's predominance should be treated as a national security issue. Losing the dominant currency position puts at great risk the dollar's valuation resiliency and the international appeal of dollar denominated debt (currently two thirds of all foreign held reserves are denominated in dollars or dollar denominated debt). This would ultimately impact the US ability to further finance its growing debt—a debt often used as an economic stimulant and a means to help finance the defense budget, as well as diplomatic interests around the world. Furthermore, major imported commodities that are denominated in dollars, such as oil, would likely become valued in another currency, adversely affecting the dollar's purchasing power of such commodities and further adding to a growing US trade deficit.

Historical Perspective: The Sterling-Dollar Transition

The transition between the sterling and the dollar is significant for two reasons. First, it is the most recent such reordering of the international financial system. Second, according to Eichengreen, based on the role of an international currency as a store of value for central banks and governments, it is the only such transition in history.[17]

---

[12] Benjamin J. Cohen, "Currency and State Power," Presented at a conference to honor Stephen D. Krasner, Stanford University, (December 4, 2009): 4.

[13] Susan Strange, *States and Markets, (*(London: Pinter Publishers, 1994): 24-25.

[14] Cohen, "Currency and State Power," 21.

[15] Barry Eichengreen, "Sterling's Past, Dollar's Future: Historical Perspectives on Reserve Currency Competition," 2.

[16] Krugman, "Vehicle Currencies and the Structure of International Exchange," 523.

[17] Barry Eichengreen, "Sterling's Past, Dollar's Future: Historical Perspectives on Reserve Currency Competition"

Chinn and Frankel provide a useful summary of this transition, which began in the late nineteenth century and lasted until the conclusion of World War II. The United States economy surpassing the British economy in size was the first key event in the transition. This occurred in 1872, but the United States lacked a robust financial system until the creation of a central bank in 1913.[18] During World War I, the United States and the United Kingdom change roles in terms of debtor and creditor and trade balances. The United Kingdom became a net debtor, while the United States assumed the role of net creditor as its exports surpassed those of the United Kingdom in 1915.[19] Despite the dollar's emergence and growing role in international trade and finance, the level of foreign-owned liquid sterling assets was twice that of the dollar as late as 1940, but by 1945 the currencies reserve positions were reversed.[20] This paints a picture of a slow shift in the underlying structure conditions, which were necessary, but not sufficient for the transition. The system was only tipped in the dollar's favor through the crisis presented by the Second World War.

Analysis of the Sterling's Economic Foundation

Various estimates of economic size have the United States surpassing the United Kingdom before the beginning of the 20th century. As stated, Chinn and Frankel put the exact year as 1872. Table 1 shows that the United States had the largest economy and the fastest rate of growth throughout the first half of the twentieth century. The most notable aspect of this data is the dramatic growth of the United States' economy relative to the other nations. Despite having become twice the size of the British economy by 1913, the dollar did not claim the primary role in the international economy until the end of World War II. This is not unexpected. Having a relatively large economy was a necessary, but not sufficient, condition for a nation's currency to achieve a primary international role.

Table 1 - GDP (billions of 1955 US dollars)

Year	United States	United Kingdom	France	Germany
1899	59	34	14	29.3
1913	97	42	16	37.5
1929	168	42	25	40.5
1937	171	50	22.4	46.5
1950	294	54.7	32.4	31.8

Source: Alfred Maizels, *Industrial Growth and World Trade* (Cambridge: Cambridge University Press, 1963), 531.

The data appear to support Rey's finding that GDP is not the primary factor in determining the internationalization of currency. It may also reflect the inertia of incumbency due to the self-reinforcing tendencies of holding the predominant position. Chinn and Frankel note that part of the explanation lies in the fact that the United States' financial system was not properly developed until

[18] Chinn and Frankel, "The Euro May Over the Next 15 Years Surpass the Dollar as Leading International Currency," 1.

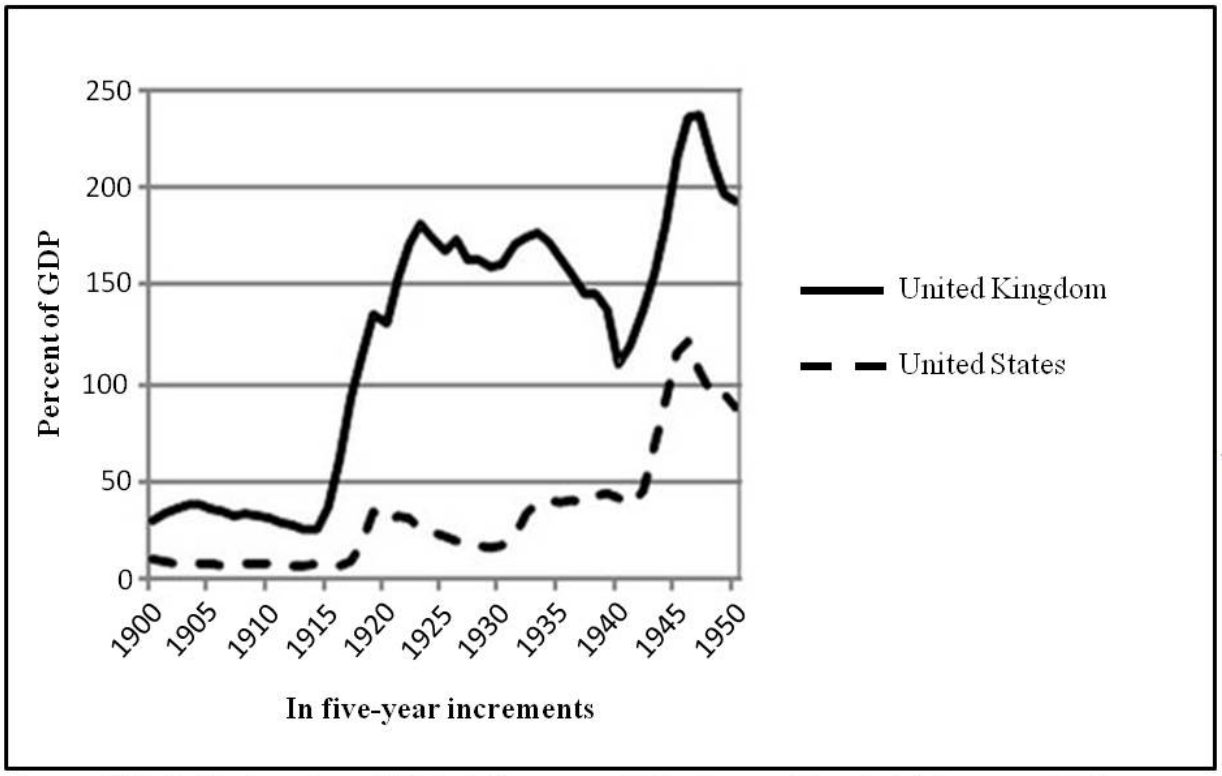
[19] Ibid.

[20] Ibid.

the creation of the central bank in 1913. Even with this condition met, it would take an additional 30 years and the events of World War II for the dollar to claim the top spot.

One explanation for the slow relative growth of the United Kingdom's economy, compared to the United States can be found in each nation's debt to GDP ratio. Figure 1 shows that the United Kingdom surpassed the 90% threshold identified by Reinhart and Rogoff in 1917, exceeding 200% briefly from 1945 thru 1948. As expected, this correlates with a slower rate of economic growth. However, as the data in table 1 show, the United Kingdom's economy grew more than the United States' from 1929-1937, during the Great Depression. This serves to undermine a notion of a causative link between high levels of debt to GDP and slow economic growth. However, there are signs that the levels of debt carried by the United Kingdom were eroding international confidence in the sterling as a store of value.

Figure 1 – Percentage of Government Gross Debt to GDP Ratios (US and UK)



Source: U.K. Public Spending, "UK Total Government Debt Current_Historical As Percent GDP," http://www.ukpublicspending.co.uk/uk_national_debt (accessed June 3, 2010); U.S. Government Spending, "US Federal Debt As Percent of GDP," www.usgovernmentspending.com (accessed June 3, 2010).

The dramatic increase in British debt coincides, not unexpectedly, with the transition of the nation's net investment position. In the years leading up to World War I, The United Kingdom maintained a current account surplus despite a persistent trade deficit.[21] This is due to large and growing income

[21] Laney, "The Reserve Role of the Dollar and the United States as Net Debtor," 5.

receipts from overseas investments, which were reinvested overseas annually.[22] These long-term loans to the rest of the world kept the United Kingdom's net investment position positive, a condition that would change during World War I. During the war, the United Kingdom transitioned to a net debtor while the United States transitioned to a net creditor due in large part to British borrowing to fund the war.[23] While the British current account recovered during the 1920s, the deficits returned in the 1930s to combine with defaults on debt, and declining values of overseas assets, eroding the nation's net worth.[24] The existing debt, defaults on current obligations, and persistent current account deficits resulted in the erosion of confidence among investors, leading them to diversify their assets by selling off their sterling reserves.

Eichengreen points out that there was a perceptible shift occurring in reserve currency allocation during the interwar years. He notes that the dollar's increasing role in trade as a unit of account and in payments contributed to international diversification in reserve currency holdings, with the sterling holding a 57% share and the dollar rising to 19% in 1928.[25] This is in line with estimates from Chinn and Frankel that the level of foreign-owned liquid sterling was double that of dollars as late as 1940.[26] However, despite high levels of debt and sustained current account deficits, the sterling maintained its leading international role.

Rey's hypothesis was that trade volume was the key determinant in the internationalization of currency. Matching this with Krugman's finding that the process of transition would be catastrophic for the incumbent, it would follow that the sterling would give way to the dollar rapidly following the United States' assumption of the top place in trade volume. Table 2 shows the United States gaining the largest share of world trade volume sometime between 1913 and 1928. Yet, this only led to slight diversification away from the sterling, not a catastrophic collapse.

Table 2 – Percent Share of World Trade

Year	United States	United Kingdom	France	Germany
1890	9.8	22.4	10.2	10.3
1913	12.9	15.5	7.3	12.1
1928	17.3	13.7	6.1	9.3
1937	16.0	14.1	4.8	8.3

Source: Simon Kuznets, *Modern Economic Growth* (New Haven: Yale University Press, 1966), 306-308.

A partial explanation for the lack of a collapse might be the relative value of each nation's exports as displayed in Table 3. According to these data, while the United States accounted for the largest share of world trade (ie, total value of exports *plus* imports) in 1928, in 1929 British exports were still

[22] Roderick Floud and Donald McCloskey, *The Economic History of Britain Since 1700: Volume 2: 1860 to the 1970s,* (Cambridge: Cambridge University Press, 1981), 289.

[23] Chinn and Frankel, "The Euro May Over the Next 15 Years Surpass the Dollar as Leading International Currency," 1.

[24] Floud and McCloskey, The Economic History of Britain Since 1700, 300.

[25] Eichengreen, "Sterling's Past, Dollar's Future," 9.

[26] Chinn and Frankel, "The Euro May Over the Next 15 Years Surpass the Dollar as Leading International Currency," 1.

slightly more valuable. Therefore, evaluation of the trade role may need to balance volume and value.

Table 3 - Value of Merchandise Exports (millions of 1990 US Dollars)

Year	United States	United Kingdom
1870	2,495	12,237
1913	19,196	39,348
1929	30,368	31,990
1950	43,114	39,384

Source: Angus Maddison, *The World Economy* (Organization for Economic Cooperation and Development, 2007), 360.

It should be noted that the value of the United States' exports was increasing from 1913-1929, while that of Britain were falling over the same period. This leads to the inference that the value of United States exports overtook those of Britain much earlier than the 1950 data can confirm. Yet it was still at least another 15 years before the dollar would surpass the sterling as an international currency.

From the 1870s through 1939, the economic balance of power shifted from The United Kingdom to the United States. It began with the United States economy becoming the world's largest. As the United States developed its financial institutions, the dollar began to play an important role in the international system. During World War I, the two nations exchanged their net investment positions, with the United Kingdom becoming a net debtor nation and the United States becoming a net creditor. The high levels of British debt and persistent deficits contrasted with the relative economic health of the United States, which slowly translated into patterns of international trade. However, the sterling maintained its role even after the United States held the dominant role in international trade. It took another world war to effect the change.

These slow foundational changes resulted in conditions where British liquid assets and exports were insufficient to finance their war effort.[27] In addition, the United States would not loan it money because it had stopped paying interest on debt from the First World War.[28] The loss of investor confidence resulted in an unwillingness to provide further loans. The United Kingdom was forced to deplete their reserves and to sell its illiquid assets under unfavorable terms.[29] The loss of these assets denied the United Kingdom the income that had kept its current account balance positive for decades and later, at least sustainable. Finally, after the Second World War crippled the United Kingdom's economy, the dollar replaced the sterling as the dominant international currency. This transition in economic power would translate into changes in state power as illustrated by the following two examples.

[27] Floud and McCloskey, The Economic History of Britain Since 1700, 306.

[28] Ibid.

[29] Ibid.

Bretton Woods – An Example of Structural Power

The creation of the Bretton Woods System during World War II provides an example of structural power and the role of economic strength as its foundation. American and British policy makers developed a joint plan for post war monetary arrangements that was adopted by 44 nations at the 1944 Bretton Woods conference.[30] The fact that the United States and the United Kingdom developed a plan that was subsequently adopted by the international community demonstrates that those two nations possessed structural power, or the ability to shape the framework of international relations. They used this power in an attempt to create an international system that reduced trade barriers, promoting free trade as a way to raise standards of living, create interdependencies, and cement post war peace through global institutions, including the International Monetary Fund (IMF) and the World Bank.[31] The system attempted to lower trade barriers by reconciling exchange rate stability and domestic economic autonomy by creating an explicit code of conduct for the international monetary system and institutional controls centered on the IMF.[32] Because the United States possessed the largest economy, it held the largest share in the IMF stabilization fund intended to finance balance of payment deficits, reconstruction and long-term development.[33] In controlling the largest share of these institutions, the United States benefited greatly through an increased ability to control the behavior of other nations in the international system. The Suez Crisis demonstrates the importance of this power to a nation pursuing its national interests.

The Suez Crisis – Lost Autonomy

When Egyptian President Gamal Abdel Nasser nationalized the Suez Canal on July 26, 1956, he triggered an international crisis that demonstrated the importance of autonomy in international relations and made clear that the United Kingdom had lost a measure of theirs. In the days following the nationalization, British Prime Minister Anthony Eden stated that the incident was a vital national interest because 80% of Western Europe's oil and commerce between the United Kingdom, India, Australia, and British colonies passed through the canal.[34] The British collaborated with the French and Israelis on Operation MUSKETEER, a military operation launched on November 5th to seize the Suez Canal.[35] However, significant reserve losses and the economic impacts of oil shortages combined to cripple the British effort.

The action had cost the British $400 million in reserves by the end of the month and the United States would not support aid from international institutions without a complete withdrawal of forces.[36] Britain did not have an alternative source of funds. The United States controlled its own

---

[30] Oatley, International Political Economy, 225.

[31] Daniel Yergin and Joseph Stanislaw, *The Commanding Heights: The Battle for the World Economy,* (New York: Free Press, 2008), 387-388.

[32] Oatley, International Political Economy, 225.

[33] Ibid., 227-228.

[34] Diane B. Kunz, *The Economic Diplomacy of the Suez Crisis,* (Chapel Hill: The University of North Carolina Press, 1991): 79.

[35] Ibid., 117.

[36] Ibid., 138, 150.

markets as well as the IMF and World Bank.[37] At the command of the United States, the United Kingdom was forced to recant an action it had labeled a vital national interest because it had run out of money. A great power must be able to act unilaterally to protect its national interests and the United Kingdom had lost this capacity with the loss of it economic dominance. Britain could forego American approval and friendship, but could not forfeit American money.[38]

Lessons From the British Experience

This transition illustrates a number of important points. Overall, it demonstrates a synthesis of Kennedy's and Ferguson's theories. The decline of the British Empire with the sterling as the dominant international currency was the culmination of over 50 years of slowly shifting economic fundamentals. The Suez crisis ultimately revealed that a shift in the balance of power had occurred between the UK and the US. The next important point is that despite high levels of debt and persistent current account deficits, the international community continued to provide financing to the United Kingdom. This continued despite the existence of a nation with a larger economy and an equal, or greater, role in trade. This reinforces Krugman's finding that once a currency becomes the leading international currency its role is self-reinforcing. The collapse in the face of a crisis may indicate that he was also correct in his assessment that a currency's fall from the top spot would be catastrophic. A final important finding is that the British collapse followed the government's sale of its illiquid income producing assets. The loss of these assets prevented the United Kingdom from retaining its position of global leadership. In the end, the reasons for the collapse of the British Empire and the sterling are complex, but the primary lesson appears to be that through excessive reliance on deficit spending, the government robbed itself of the ability to function autonomously when it needed to.

While this overview is useful in illustrating these points, it is important to acknowledge the context of that transition. American isolationism and the Great Depression may have slowed the process. These factors probably pushed investors to the sterling, which had the trust of the international community. This would be similar to the reaction of the international community to the latest financial crisis.[39]

Prospects for the Dollar

Analysis of the Dollar's Economic Foundation

The current position of the United States appears to be different from that faced by the United Kingdom a century ago. Unlike the position of the United Kingdom at the beginning of the 20th century, the United States still has the world's largest economy. Table 4 lists the ten largest economies measured by GDP. Only the Eurozone (European Union countries that also use the euro as a common currency) is close to matching the United States' economic size.

---

[37] Ibid., 193

[38] Ibid.

[39] Eichengreen, "The Dollar Dilema," 55-56.

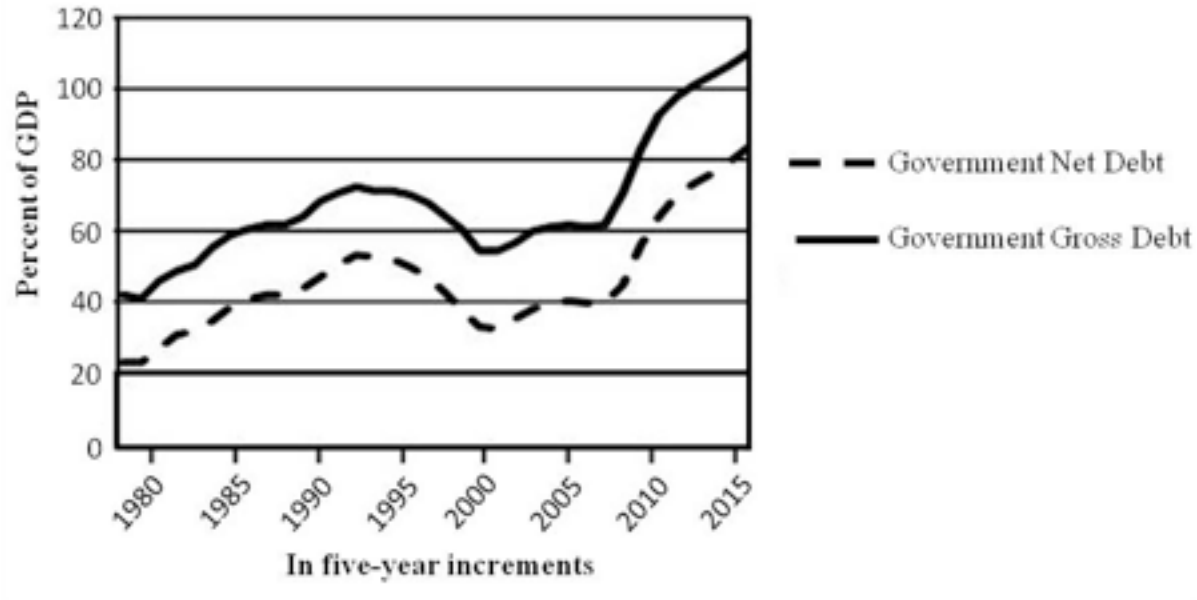
Table 4 - Top Ten World Economies (including Eurozone)

Rank	Country	2008 GDP (millions of U.S. dollars)	% of World GDP
1	United States	14,093,310	23.3%
2	Eurozone	13,580,866	22.4%
3	Japan	4,910,840	8.1%
4	China	4,326,996	7.1%
5	Germany	3,649,494	6.0%
6	France	2,856,556	4.7%
7	United Kingdom	2,674,057	4.4%
8	Italy	2,303,079	3.8%
9	Russian Federation	1,679,484	2.8%
10	Spain	1,604,235	2.6%

Source: The World Bank, "World Bank Data Catalog." http://data.worldbank.org/data-catalog (accessed June 3, 2010).

As reflected in figure 2, another difference is that the United States just crossed the threshold of 90% debt to GDP ratio in 2010. As was demonstrated in the British example, it is possible for a lead nation to endure this level for decades. However, the rising levels of debt projected by the IMF are cause for concern, as it may cause investors, both private entities and foreign governments, to seek other destinations for their capital. Examination of the trade roles provides further insight into the dollar's economic foundation and identifies additional concerns.

Figure 2 – Percent of US Government Debt to GDP Ratio (Projected Through 2015)



Source: International Monetary Fund, "World Economic Outlook Database April 2010," http://www.imf.org/external/pubs/ft/weo/2010/01/weodata/index.aspx (accessed August 15, 2010).

As the British case demonstrated, it is prudent to consider both trade volume and export values to analyze the strength of the United States and the dollar. According to table 5, the United States still accounts for the greatest share of the world's trade volume (exports plus imports). However, six of the top ten nations, in terms of trade volume, are members of the Eurozone. From the table, their combined share of world trade volume is more than twice that of the United States, which, according to Rey, is the key determinant of the dominant international currency. However, the British case showed that the United States had passed the United Kingdom in terms of trade volume by 1928 without causing the sterling to collapse.

Table 5 - 2009 Percent Share of World Merchandise Trade

Rank	Country	2009 Share of World Volume
1	United States	10.6%
2	China	8.8%
3	Germany	8.2%
4	Japan	4.5%
5	France	4.1%
6	Netherlands	3.8%
7	United Kingdom	3.3%
8	Italy	3.2%
9	Belgium	2.9%
10	Republic of Korea	2.7%

Source: World Trade Organization, *World Trade 2009 Prospects for 2010* (Geneva: WTO, March 2010), 10.

Table 6 - Value of Merchandise Exports (US dollars)

Rank	Country	2009 Export Value
1	China	$1,204,000,000,000
2	Germany	$1,159,000,000,000
3	United States	$1,046,000,000,000
4	Japan	$542,300,000,000
5	France	$472,700,000,000
6	Netherlands	$417,600,000,000
7	Italy	$412,900,000,000
8	Republic of Korea	$373,600,000,000
9	United Kingdom	$357,300,000,000
10	Canada	$323,400,000,000

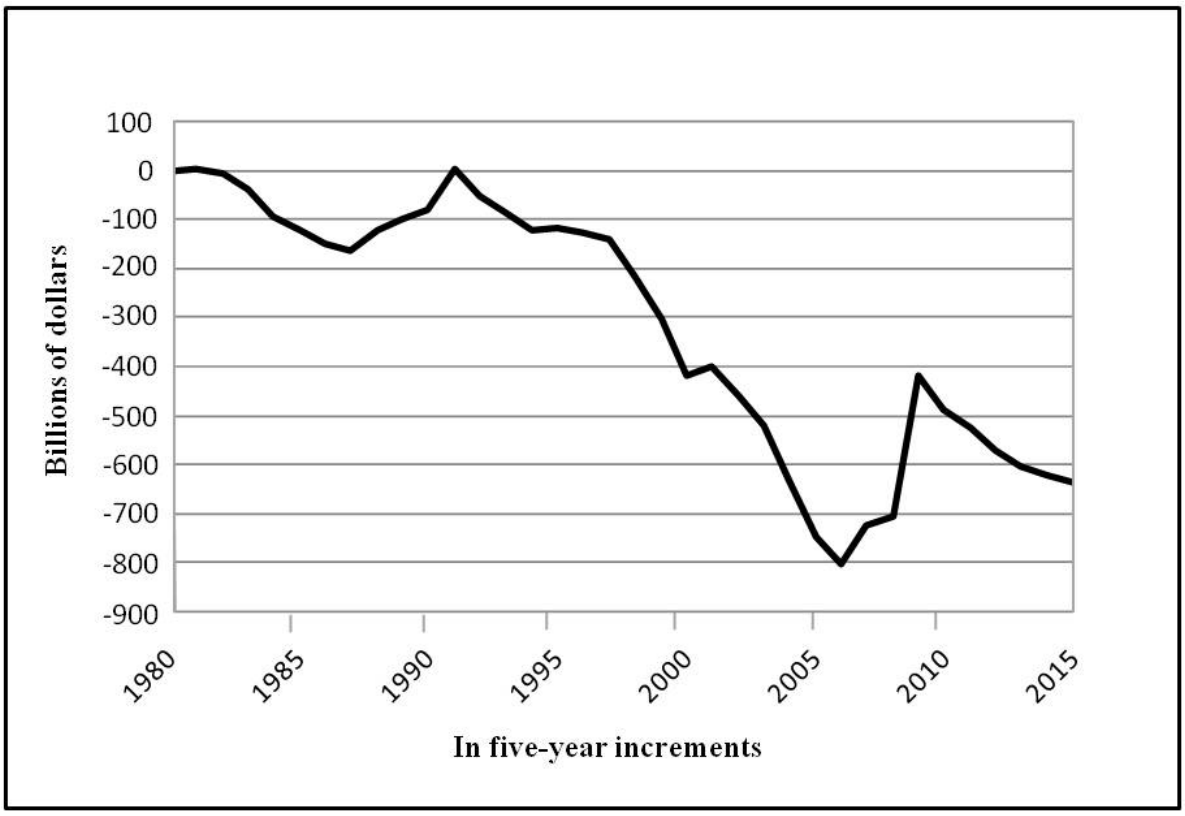
Source: CIA Factbook Country Comparison: Exports," (accessed September 10, 2010). https:/www.cia.gov/library/publications/the-world-factbook/rankorder/2078rank.html

Table 6 shows that the United States does not hold the lead in terms of the value of its exports either. It currently sits third behind China and Germany. The fact that Germany is in front of the United States in terms of export value means that the Eurozone leads the United States in both measures of trade.

At this point in the evaluation, there are indicators that the dollar may be vulnerable. The economic foundation of the Euro is nearly the same size as the United States, and the Eurozone accounts for more international trade in terms of both volume and value. Combined with the high levels of debt to GDP in the United States, which are expected to correlate with increasing inflation and slow economic growth, it is reasonable to expect investors may begin looking to diversify their holdings as they did during the interwar period. Another factor, which will erode investor confidence in the dollar as a store of value, is a growing trade deficit that would put downward pressure on the dollar if investors stop buying the currency as a reserve. This may lead to a rapid collapse as predicted by Krugman's theory.

The data show that the United States current account is increasingly negative which will heighten the vulnerability of the dollar if it follows current projections. Figure 3 shows a sharply negative projection of the United States' current account between 1998 and 2006. The data show that the deficit nearly quadrupled from $213 billion in 1998 later bottoming at $803 billion in 2006, before a slight rebalancing in 2007 and 2008.

Figure 3 - United States Current Account Balance of Payment Data (billions of US dollars)



Source: International Monetary Fund, "World Economic Outlook Database April 2010," http://www.imf.org/external/pubs/ft/weo/2010/01/weodata/index.aspx (accessed August 15, 2010).

The IMF projection for the 2010 current account deficit is $487 billion, which is still more than double the 1998 level and reverses a three-year trend of reduced current account deficits.[40] While the nation's deficits have come down from their peak in 2006, at nearly 5% of GDP they are too high to control the rising debt and are projected to continue increasing following 2010. A deficit to GDP ratio of 2% would likely prove to be a sustainable level, as it would allow GDP to grow, on average, at a faster rate than debt.[41] This would equate to reducing deficits at 1998 levels, which may or may not be possible without serious tradeoffs.

In order to understand what is possible, it is necessary to understand why the trade deficit is as large as it is. There are two explanations for the emergence of the current global imbalance. The first offered by Ben Bernanke is the "global savings glut," which is the result of the developing world's transition from net borrower to net lender.[42] His argument is that developing countries lost some capacity to borrow because of financial crises in the 1990s. The long-term impact of these crises is that developing nations became less willing to borrow and run budget deficits. They have instead turned to accumulation of foreign exchange reserves by their central banks as a method of national savings. Finally, Bernanke holds that the rise in oil prices has resulted in an abrupt increase in revenue and saving for oil exporting nations. He argues that this excessive savings was attracted to the United States because of the technology boom in the 1990's, the maturity and safety of its capital markets, and the unique role of the dollar as a reserve currency.

The second explanation is the "money glut" as advanced by Martin Wolf.[43] In this view, the United States monetary excess causes low nominal and real interest rates making credit attractive and available to consumers. This has the effect of lowering savings while increasing spending which absorbs imports. The dollar then loses value against floating currencies, but pegged currencies are kept low relative to the dollar by foreign currency intervention. In the end, this view argues that excess money creation by the United States forces the rest of the world to invest in the dollar as a foreign exchange reserve in order to control excessive demand and inflation. As Wolf points out, understanding which view is correct is important; if the savings glut is correct, the adjustment can be controlled, but if the money glut is more accurate then the adjustment will come at the cost of monetary stability.[44]

Are the Global Imbalances Sustainable?

While there seems to be consensus that the dollar will inevitably lose its predominance, there is wide disagreement on the process of transition and the end state. This is likely due to the uncertainty regarding the true meaning of the United States current account deficits and overall levels of debt. As previously stated, Kennedy and Ferguson have opposing views on the length of a possible

---

[40] *World Economic Outlook Database* at the International Monetary Fund website, https://www.imf.org/external/pubs/ft/weo/2010/01/weodata/index.aspx, (accessed June 3, 2010).

[41] Michael Mussa, "Exchange Rate Adjustments Needed to Reduce Global Payment Imbalances," In *Dollar Adjustment: How Far? Against What?*, by C. Fred Bergsten and John Williamson, (Washington, D.C.: Institute for International Economics, 2004), 118.

[42] Ben Bernanke, "The Global Savings Glut and the U.S. Current Account Deficit" (The Sandridge Lecture, Virginia Association of Economics, March 10, 2005).

[43] Martin Wolf, *Fixing Global Finance,* (Baltimore, MD: The Johns Hopkins University Press, 2008) 109.

[44] Ibid., 110.

transition. Chinn and Frankel state that the Euro could replace the dollar as a single dominant currency as early as 2015.[45] However, their conclusions were drawn in 2008, and the ongoing European debt crisis will likely impact investor confidence and, at the least, extend that timeline. On the other hand, Eichengreen sees the potential for two or three currencies to share the reserve role in the market in the 2020 – 2040 timeframe.[46] In addition to the uncertainty surrounding the United States' debt level, this disagreement also reflects the lack of numerous historical references.

As stated earlier, the United States current account deficit is not considered indefinitely sustainable along the current trajectory. The question is how much higher can deficits and debt go before an adjustment occurs. Martin Wolf contends that the imbalances are sustainable as long as creditors are willing to finance the United States.[47] What his statement implies is that the creditor nations are making a deliberate choice to buy the dollar and hold it as a reserve. This is in line with the example provided by continuing support for the sterling in the first half of the twentieth century. Therefore, to understand what is sustainable, it is necessary to understand why they continue investing in the dollar.

The theory maintains that the capital will flow to the highest rate of return, seeking the best store of value. The Congressional Research Service offers reasons this might be the case for the United States and the dollar. They are that the United States has enjoyed greater productivity growth than most of the world since the mid 1990's, higher interest rates due to the low level of domestic savings combined with deficit spending, and the theory of diminishing returns which in this case applies to developed countries' need to invest abroad for efficiency reasons.[48] The problem with this is that the returns are likely to get worse due to depreciation of the dollar. If investors are only seeking a high rate of return, they are likely to abandon the dollar.

Paul Krugman argues that the dollar must depreciate. This is the result of his view that the trade deficit is not sustainable, that closing it requires a redistribution of world spending which requires a fall in relative prices of goods produced by the United States.[49] This is nothing different from a normal balance of payments adjustment. The question revolves around the speed of this depreciation.

The dollar was depreciating steadily at a rate of 3-4% annually from 2002-2006, but then declined by 10% in 2007.[50] The trend has been reversed as investors have flocked to the dollar during the recent financial crisis in search of a safe haven. As the world economy recovers, there is no reason to believe that the dollar depreciation will not continue. The crucial question to Krugman "is whether the dollar must eventually depreciate at a rate faster than investors now expect."[51] It is reasonable to infer that the investors expect and accept a rate of depreciation at or below 3-4% annually as they

---

[45] Chinn and Frankel, "The Euro May Over the Next 15 Years Surpass the Dollar as Leading International Currency," 18.

[46] Eichengreen, "Sterling's Past, Dollar's Future," 21.

[47] Wolf, Fixing Global Finance, 149.

[48] Congressional Research Service, *Is the U.S. Trade Deficit Caused by a Global Saving Glut?* (RL33140, Washington, DC: Government Printing Office, June 20, 2007).

[49] Paul Krugman, "Will There Be a Dollar Crisis," *Economic Policy*, (July 2007), 438.

[50]Congressional Research Service, *The Depreciating Dollar: Economic Effects and Policy Response*, (RL34582, Washington, DC: Government Printing Office, July 17, 2008), 1.

[51] Paul Krugman, "Will There Be a Dollar Crisis," *Economic Policy*, (July 2007), 439.

did from 2002-2006. What is not clear is if they will accept a 10% decline like the one that emerged in 2007. Krugman argues that if investors fail to account for the required devaluation there will be a 'Wile E. Coyote' moment were they look down and realize there is nothing supporting their investment.[52] The question then becomes whether the dollar must depreciate faster than the 3-4% rate.

Krugman evaluates two scenarios for dollar depreciation that help answer this question. The first scenario occurs over 20 years at an annual depreciation rate of 1.75%.[53] This rate of depreciation is clearly under the 3-4 percent depreciation levels of 2002-2006. The problem with this rate is that after accounting for growth and valuation adjustments, it results in a net external debt to GDP ratio of 118%. As previously discussed, that level of external debt to GDP has never been sustained by a large nation, which makes it a dangerous course. In addition, Krugman finds that it might result in foreign ownership of more than one-third of the United States' capital stock.

The second scenario occurs over 10 years at an annual rate of 3.5%.[54] The resultant net external debt to GDP ratio in this scenario, after accounting for growth and valuation adjustments, is only 58%. This scenario also avoids the problem of large-scale foreign ownership of the nation's capital stock. This rate of depreciation is still within the range that was sustained from 2002-2006, indicating that it may be possible to close the United States current account deficit without a major dollar crisis. For this to happen, investors would have to expect and accept the dollar's depreciation and the dollar would have to depreciate no faster than Krugman's projected rate. While it appears that the current global imbalances are not sustainable, it seems plausible that an adjustment does not mean the end of the dollar as the predominant international currency. The fact that investors have already accepted the necessary level of depreciation over a five-year period indicates that they would be willing to accept it over the longer ten-year period in Krugman's model. The reasons for this could be that they are more concerned with the ability to quickly retrieve their investment than they are with pure value retention. If this is the rationale for investment in the dollar, then this is where the true vulnerability of the dollar can be found.

A Plausible Future for the Dollar?

If investors are willing to accept some annual depreciation in exchange for the ability to quickly liquidate their reserves and intervene in a crisis, it should be asked whether there are investors that hold such a large share of United States securities that they alone pose a risk to the dollar's status. It is impossible to know exactly what scenario might emerge to cause the dollar to lose its place as the dominant international currency, but it is certainly possible to evaluate existing vulnerabilities.

Concern that China will seek to liquidate its large share of dollar holdings makes the unlikely assumptions that the rest of the world can absorb their share and that they are willing to accept significant losses as the value of the dollar plummets during the selloff. It could also result from some unforeseen crisis such as another world war, as was the case for the United Kingdom. However, because the United States is reliant on the international community to fund its current budget deficit, the real problem may reside in the economic health of those nations.

---

[52] Ibid., 440.

[53] Ibid., 445.

[54] Ibid.

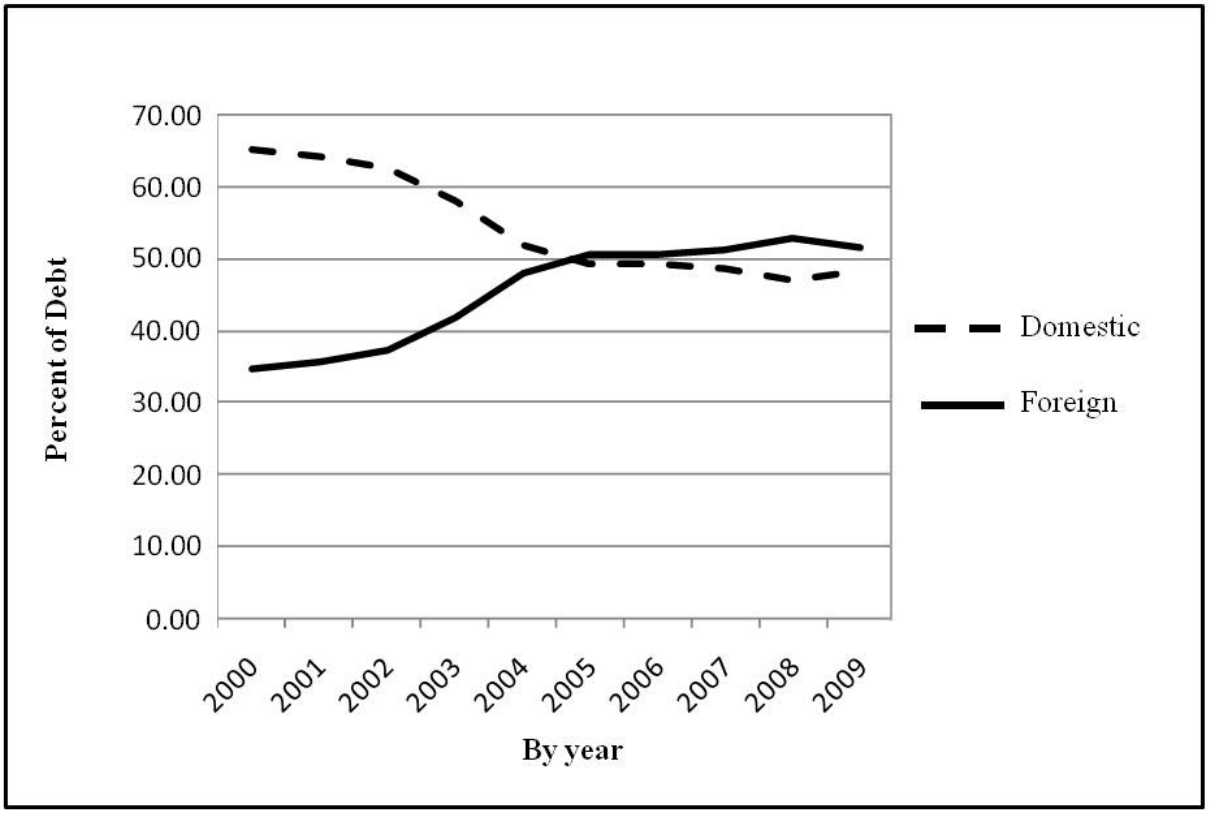
Table 7 shows the four largest holders of United States Treasury securities. This data shows that China is currently reducing its holdings in the dollar, while Japan and the United Kingdom are increasing theirs. Over the last year, Japan has increased its holdings by $95.4 billion, while the United Kingdom has increased its dollar holdings by $271.4 billion. The United States' reliance on these nations to fund its budget deficit is reason to examine their economic foundation. Their domestic economic crisis could quickly affect the United States if they are unable to continue purchasing its debt, or if they are forced to liquidate dollar holdings in response.

Table 7- Major Foreign Holders of US Treasury Securities (billions of US dollars)

Country	July 2009	January 2010	July 2010
China, Mainland	915.8	889	843.7
Japan	708.2	765.4	803.6
United Kingdom	90.8	208.3	362.2
Oil Exporters	211.8	218.4	223

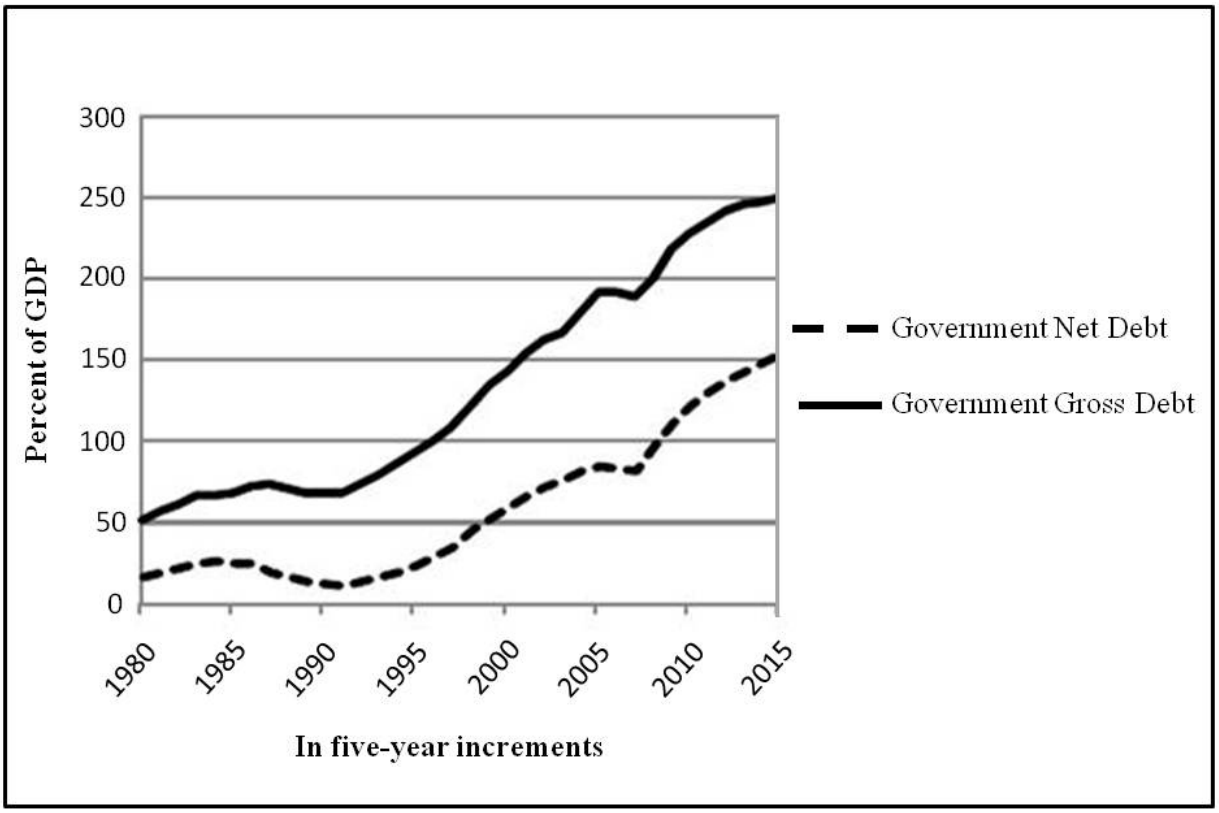
Source: United States Treasury, "Treasury International Capital System - Home Page," http://www.ustreas.gov/tic (accessed September 10, 2010).

Figure 4 - Ownership of US Debt



Source: United States Treasury, "Treasury Bulletin September 2009," http://www.ustreas.gov/tic (accessed June 3, 2010).

Figure 5 - Japanese Debt to GDP Ratios

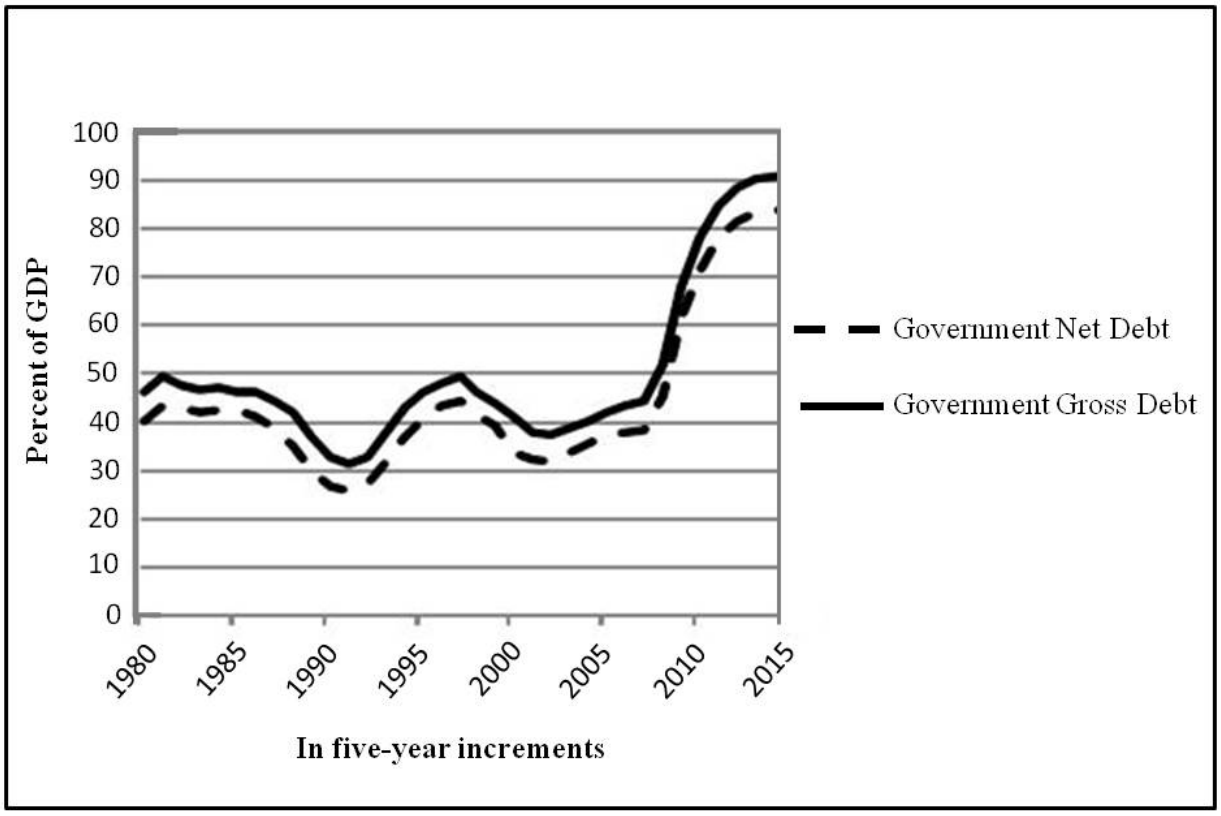


Source: International Monetary Fund, "World Economic Outlook Database April 2010," http://www.imf.org/external/pubs/ft/weo/2010/01/weodata/index.aspx (accessed August 15, 2010).

This comes at a time when the United States is increasingly dependent on foreign capital to finance its budget deficits and as a result debt is increasingly owned by foreign investors, both private investors and governments. Figure 4 shows that as a percentage, more than half of the United States public debt is owned by foreigners. However, in real terms, both foreign and domestic investors have been increasing their ownership in recent years. The significance of this is that the United States in increasingly reliant on external sources of capital to fund its budget deficits. Because domestic investors have also increased their purchases of debt, it is not certain that they would be able to offset a rapid international selloff of United States securities. Nor is it likely, that they would be willing to invest in a security that was rapidly losing value. Two potential scenarios that could lead to the fall of the dollar present themselves in this data.

Japan's current role as a major holder of United States debt, combined with its own debt concerns may prove to be the spark that leads to the dollar's loss of international predominance. Figure 5 shows that Japan has a serious structural problem regarding its debt level. Its gross public debt to GDP ratio has been above Reinhart and Rogoff's 90% threshold since 1995, and is projected to reach and surpass levels experienced by The United Kingdom during World War II. Even more concerning, is the projected growth in the net debt to GDP ratio, reaching 150% by 2015. If Japan is forced to sell off its reserves to deal with payment issues, as the United Kingdom was forced to during World War II, it might lead to Krugman's Wile E. Coyote moment. This scenario is more likely when Japan's falling savings rate is considered. Furthermore, the household savings rate in Japan has been falling from 15% in the 1980s to 2% in 2009 which is threatening Japan's net savings

Figure 6 - United Kingdom Debt to GDP Ratios



Source: International Monetary Fund, "World Economic Outlook Database April 2010," http://www.imf.org/external/pubs/ft/weo/2010/01/weodata/index.aspx (accessed August 15, 2010).

surplus and, in turn, its ability to export capital.[55] A Japanese liquidation of dollar assets would put downward pressure on the dollar. This in turn, would reduce the value of dollar holdings around the world, potentially causing other investors to begin selling their dollar securities before the bottom falls out. This would be the equivalent of a bank run on an international scale.

The United Kingdom's economic health poses a similar problem. Figure 6 illustrates that, while their debt levels are not as high as Japan's, they are predicted to rise above 90% of GDP within the next five years. The most concerning aspect of the United Kingdom's debt is the rapid rate of growth following 2007, doubling by 2012. As the United Kingdom faces its rapidly growing debt, likely accompanied with higher interest payments, it may not be able to purchase additional United States debt. As Table 7 showed, the United Kingdom has increased its holdings of United States Treasury Securities by $271.4 billion over the last year. This has allowed the United States to continue financing the wars in Iraq and Afghanistan, as well as the large economic stimulus. However, an inability to purchase additional debt is not the real problem for the United Kingdom, much like the scenario with Japan; the problem emerges when the United Kingdom is forced to sell its reserves to cover its own payments or to intervene in a crisis that threatens its economy.

[55] Martin Feldstein, "Japan's Savings Crisis," Project Syndicate, http://www.project-syndicate.org (accessed October 13, 2010).

A resurgence of the sovereign debt crisis that hit Europe earlier this year could trigger such a scenario. Based on data in table 8, five high-risk nations owe the United Kingdom a total of $418 billion. Three fourths of this amount is owed by Spain and Ireland, nations who have significant debt issues of their own.

Table 8 - Debt Owed to the United Kingdom (billions of US dollars)

Country	Debt to United Kingdom
Ireland	188
Spain	114
Italy	77
Portugal	24
Greece	15

Source: Bank for International Settlements, 2010

Spain and Ireland have both experienced setbacks in their efforts to avoid future defaults. The Irish have announced an initiative to spend billions to prop up its banking sector while Moody's downgraded Spain's credit rating on September 30, 2010 over concerns about its current financial condition and prospects for growth.[56] A default by either of these nations on obligations to the United Kingdom might force the United Kingdom to liquidate a significant portion of its dollar holdings. In either case, a major selloff of dollars by one of the top three holders could cause a panic, as investors would seek to sell their holdings before the value plummets.

Impacts to National Security

Just as it is impossible to predict exactly what the future of the dollar holds, it is impossible to predict exactly the second and third order effects of a dollar collapse. However, the falling value of the dollar would have important consequences because of the United States' continued reliance on deficit financing. The inflow of foreign financing would be dramatically, if not wholly, reduced as the value of the dollar falls. Therefore, the United States would have to pay higher interest rates to fund future debt to offset the increasing uncertainty about its future value; this would place a restrictive constraint on future government spending. Any hope of covering this spending shortfall by increasing revenue through taxation is also unlikely to succeed in the short-term because of potential impacts to the domestic economy. Eventually, the economy would recover as the weaker dollar makes United States exports more affordable for the rest of the world.

Such a crisis would force the United States Government to make immediate spending cuts due to the loss of international funding. The fiscal year 2010 budget provides an example of the risk. The

[56] Wall Street Journal World at a Glance, "World Watch – Europe," Wall Street Journal Online, http://online.wsj.com/article/SB10001424052748704483004575524032776735098.html (accessed October 1, 2010).

Congressional Budget Office (CBO) projections for fiscal year 2010 anticipate $2.175 trillion in revenue balanced against $3.524 trillion in outlays.[57] The budget deficit for 2010 is then $1.349 trillion. This accounts for nearly all of the discretionary spending for 2010, which is $1.371 trillion.[58] In other words, the United States could only fund 1.6% of its 2010 discretionary spending without borrowing from foreign governments and private investors. This means that almost any disruption to the inflow of capital from these investors would force the government to suspend governmental operations, including overseas military operations or cut entitlements such as Social Security and Medicaid. Congress would likely try to spread the spending reductions across governmental functions, but the political reality is that cutting spending on overseas military operations is easier than cutting social programs for constituents.

Even modest reductions in government spending would affect funding support for the National Security Strategy. The 2010 National Security Strategy outlines four enduring national interests – *security* of the United States, its citizens, allies and partners; *prosperity* through a growing United States economy in an open international system; respect for universal *values* throughout the world; and an *international order* advanced by United States leadership and international cooperation.[59] Each of these national interests would be adversely affected by a dollar crisis.

A key component of the national interest in security is to disrupt, dismantle, and defeat terrorism around the world.[60] The frontline of this effort is in Afghanistan and Pakistan where the United States is fighting an insurgency, working to build an effective Afghan government, and looking to increase trust and respect with the Pakistani government while supporting their capacity to target extremists.[61] It is likely that these would be among the first casualties of budget cuts, as the American public would demand the government prioritize a severe domestic crisis over the enduring war effort. Even absent calls from the public, it is unlikely the United States could find a way to continue funding the $165 billion required for wars in Iraq and Afghanistan in the face of a dollar crisis.[62] Beyond the immediate crisis, the higher interest rates that would be required on new debt following a crisis would also constrain the nation's ability to conduct future overseas military operations as it did for the British in the 1950s. Further undermining US security interests are the debt problems of our allies, who increasingly find themselves having to pit their domestic needs against the need for global security.

The remaining national interests of prosperity, values and international order would be undermined by the inability of the United States to continue funding international development institutions at current, and less than ideal levels. One policy nested within the prosperity interest is to increase investments in development in order to help developing countries grow into prosperous, democratic, and accountable states.[63] The United States' support to international institutions such as the IMF and World Bank are critical ways that the nation works toward an open international

---

[57] Congressional Budget Office, *The Budget and Economic Outlook: Fiscal Years 2010 to 2020,* (Washington, DC: Government Printing Office, January 2010), 8.

[58] Ibid.

[59] Barack H. Obama, *The National Security Strategy of the United States*, (Washington, DC: The White House, May 2010), 17.

[60] Ibid., 19.

[61] Ibid., 21.

[62] Congressional Budget Office, *The Budget and Economic Outlook*, 6.

[63] Obama, The National Security Strategy, 33.

economic system while simultaneously promoting universal values and international cooperation. The United States may not be able to maintain its leadership role in these organizations following a dollar crisis, as it will become harder to maintain a higher level of financing relative to the other members. The United States could find itself reliant on the policy interests of another nation that may not weigh universal values, democracy, and international cooperation as highly as it does.

The case for fiscal year 2010 is extreme based on stimulus spending, however, it is also a fact that the government faces. The CBO projects that annual budget deficits will fall dramatically by 2020 behind significant increases in revenue, resulting in deficit levels equal to less than half of annual discretionary spending.[64] These revenue increases are not guaranteed; there is ongoing debate regarding the expiration of the Bush tax cuts in 2012 and future growth in revenue is linked to economic recovery. If realized, this structure will reduce the United States' vulnerability, but it does not eliminate it as the reliance on external funding remains and the overall debt burden continues to increase.

Conclusion

The analysis indicates a synthesis of Kennedy and Ferguson's theories of great power decline. Economic foundations shift slowly over time, but the true frailty of the system is not apparent until a crisis tips the balance of power. Much of the United States' current international power has been derived from its economic strength, and the translation of that strength into leading roles in current international institutions such as the IMF and World Bank. However, there are indicators that this strength has turned into vulnerability due to excessive budget deficits financed by foreign nations with growingly fragile economic fundamentals.

Economists' views of international currencies and the case of the interrelated declines of the sterling and the United Kingdom indicate that there are a number of necessary conditions that can make a great power vulnerable. The loss of economic prominence—as measured in terms of GDP, gross government debt, and trade—weakened investor confidence in the sterling, while undermining its utility in the trade roles of an international currency. This resulted in diversification by central banks and private investors who replaced a portion of their sterling reserves with dollars. This reduced the inflow of foreign capital to the United Kingdom, led to its inability to continue making interest payments on debt owed to the United States. When the United States refused additional loans to Britain at the outset of World War II, it forced them to sell their gold reserves and illiquid income producing assets. In the end, the United Kingdom had relied too heavily on deficit spending supported by external sources. When these sources proved unwilling to provide further support, the United Kingdom and the sterling gave way to the United States and the dollar. This resulted in the loss of international leadership, but also lost autonomy as demonstrated by the Suez Crisis.

The United States is now following the same path as the nation's debt has grown rapidly in the midst of its own wars following the terrorist attacks on September 11, 2001. There is a long-term vulnerability in the trajectory of the United States' current account deficit and growing debt burden, which will undermine investor confidence in the dollar as a store of value. If foreign governments and private investors no longer view United States securities as a safe store of value, they will begin to diversify their reserve holdings. This combined with the United States' loss of its lead in world trade could result in the replacement of the dollar as the primary international currency. However,

[64] Congressional Budget Office, *The Budget and Economic Outlook*, 8.

the evidence indicates that investors still feel that the dollar is a useful investment, either as a store of value, or as a highly liquid asset that provides a ready means to intervene in a domestic crisis. Therefore, the United States has time to make necessary adjustments before the dollar loses its predominant role. Change will require altering federal spending priorities to restore fiscal discipline. However, investors holding the dollar for its high liquidity create a different vulnerability, with potentially more immediate consequences.

If foreign governments are holding the dollar for its liquidity, the real danger to the United States international predominance may reside in the house of cards upon which its deficit spending relies. The largest, and fastest growing, investors in United States securities are heavily indebted themselves. This leaves the country vulnerable to a crisis that it cannot control. Looming crises in those nations could result in a run on the dollar, which would force the United States Government to make an immediate budgetary decision between national security and other spending. Defense cuts would undermine national security objectives as stated in the 2010 National Security Strategy and constrain ongoing overseas military operations and the nation's leadership role in international institutions. A dollar crisis could also result in the dollar's loss of status as the leading international currency, which poses long-term implications to national security, as the US would lose a measure of its autonomy as the United Kingdom did following World War II.

Special Thanks

The authors would like to thank Mr. Tom Daze of the US Army Command and General Staff College for his invaluable technical assistance in preparing the tables and figures contained in this article.

About the Authors

Dr. David A. Anderson is a retired US Marine Corps officer. He is now a professor of Strategic Studies and Odom Chair of Joint, Interagency, and Multinational Operations at the US Army Command and General Staff College, Fort Leavenworth, Kansas, where he teaches strategic and operational studies, as well as economics. He is also an adjunct professor for Webster University, where he teaches various international relations courses including, International Political Economy and Globalization. He has published numerous articles on military, economics, and international relations related topics.

Major Neil C. Everingham is an active duty officer in the US Army. He is a recent graduate of the Advanced Military Studies Program at the Army's School of Advanced Military Studies, Fort Leavenworth, Kansas. He is currently serving in Afghanistan as an operational planner in the International Security Assistance Force Joint Command. He holds a Masters of Public Administration from Central Michigan University and a Masters of Military Art and Science from the Command and General Staff College, Fort Leavenworth, KS.

STRATEGIC INSIGHTS

Call for Papers: Weapons of Mass Effect

Submissions due: June 3, 2011

Strategic Insights, an online journal published by the Center on Contemporary Conflict at the Naval Postgraduate School, is seeking scholarly papers on Weapons of Mass Effect (WME). WME are those that cause massive psychological or economic damage or loss of life. An attack likely involved a WME if any of the following are true:

- The number of people killed is over one hundred.
- The attack devastated a large area—a square mile of a city or ten square miles in rural areas.
- The attack damaged or destroyed a critical facility, such as a power plant, a major airport, or an important government office.
- The attack disrupted everyday services enough to cause a significant reduction in quality of life.
- The attack caused significant economic losses to the target (eg, $10 billion for the United States, less for developing nations).
- A manifest "degree of terrorism"—a subjective but nonetheless present psychological or emotional impact on the population.

Strategic Insights is interested in papers that examine recorded incidents of WME and examine any policy changes they provoked and their implications for policy makers. Of particular interest are incidents that changed the way states view their national security or their relations with other states.

Submission Details: Submissions should be addressed to *SI* Editor Brent Kesler and sent in MS Word compatible format to ccc (at) nps.edu. They should range between 5,000 and 8,000 words. For more information on submission guidelines, please consult:

http://www.nps.edu/CCC/Research-Publications/StrategicInsights/submissions.html

Timeframe:

- June 3: Submissions due
- June 17: Notification of acceptance/rejection/request for revisions
- July 1: First revisions due
- July 29: Publication