American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uafp20

800 Titles but No Policy—Thoughts on Cyber Warfare

Misha Glenny & Camino Kavanagh

Version of record first published: 07 Dec 2012.

To cite this article: Misha Glenny & Camino Kavanagh (2012): 800 Titles but No Policy—Thoughts on Cyber Warfare, American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy, 34:6, 287-294

To link to this article: http://dx.doi.org/10.1080/10803920.2012.742410

American Foreign Policy Interests, 34:287–294, 2012

ISSN: 1080-3920 print/1533-2128 online
DOI: 10.1080/10803920.2012.742410

800 Titles but No Policy—Thoughts on Cyber Warfare

Misha Glenny and Camino Kavanagh

ABSTRACT Have the last few years brought the first glimpses of a cyber space arms race? Or is the Internet already a theater of cyber warfare? The whirlwind technological changes, growth, and evolution of the Internet infrastructure and networked computer systems have opened military, civilian, and industrial security breaches worldwide—an information and communications Achilles' heel especially vulnerable to hacking and malware. In response, the U.S. military has established a new Cyber Command to "patrol" the virtual world. With deterrence now an outmoded concept, what will the future look like in terms of safety, information security, individual rights, privacy, and access?

KEYWORDS cyber; cyber warfare; espionage; hackivist; networked computer technology; Stuxnet; U.S. Cyber Command

Misha Glenny is an author, broadcaster, and former BBC Central Europe correspondent, who covered the revolutions in Eastern Europe and the wars in the former Yugoslavia. He has written for many major publications around the world, including the New York Times, *the* New York Review of Books, *and* The New Yorker. *His previous books include* The Balkans, 1804–2011 *(now updated) and* McMafia: Journey through the Global Criminal Underworld. *The latter book was translated into more than 30 languages, shortlisted for the FT Business Book of the Year and the Lionel Gelber Prize for International Affairs, and is currently being developed as a TV series for Working Title films. In January 2012, Glenny was a visiting professor at Columbia University's Harriman Institute. His latest book*, DarkMarket: Cyberthieves, Cybercops and You*, has been published in more than twenty editions around the world and is on the shortlist for two major prizes. He is currently the UK's Information Security Journalist of the Year and is now working on a book about Brazil.*

Camino Kavanagh is a Ph.D. candidate at the Department of War Studies, King's College London, and a nonresident fellow with University of Toronto's Canada Center for International Security Studies, where she is focusing on grand strategy and cyber. She is also a fellow at NYU's Center on International Cooperation, where her research focuses on threats posed by organized crime and drug trafficking. Camino has more than fifteen years of experience working with the UN and other international organizations in a range of post-conflict and fragile settings around the world.

It is now a truism that most humans cannot keep up with the speed of technological development across cyber space. But the last two years have witnessed rapid advances in an area of the Internet that many may choose to engage with—cyber warfare.

Unfortunately, in the real world, our diplomatic mechanisms appear entirely inadequate for the challenge posed by militaries and intelligence agencies responsible for the growth in both defensive and offensive cyber capability.

Throughout the first decade of this century, states were largely concerned with three negative aspects of the Web and networked computer technology: cyber crime (which focused chiefly during this period on what we call "high-volume, low-impact" credit and debit card fraud); espionage, including military, political, and commercial—made notorious in particular by the sustained multiple probings of U.S. government networks by the Chinese in an operation that was dubbed "Titan Rain"; and intellectual property theft, which is a curious hybrid of considerable significance that combines aspects of cyber crime and espionage.

That is not to say that some in the Department of Defense (DoD) were completely unaware of the implications of our growing dependency on networked computer systems. As early as 1997, an internal exercise, Eligible Receiver, exposed how ill-prepared the United States was to combat cyber attacks. NSA (National Security Agency) hackers used publicly available material to successfully break into the DoD's U.S. Pacific Command Center,

the country's electricity grids, and 911 systems in nine major cities. In 1998, U.S. officials accidentally discovered that for two years someone had been probing the computer systems of the Pentagon, National Aeronautics and Space Administration (NASA), the Department of Energy, and some private universities and research labs. The DoD traced the trail of Moonlight Maze, as it was called, to a mainframe computer in the former U.S.S.R., but the precise sponsor of the attacks remained unknown and Russia denied any involvement. Several other worms targeting critical infrastructure for espionage and surveillance were discovered throughout 2003. These very clear warnings were not coherently acted upon until later.

That began to change in the spring of 2007 when Estonia suffered a series of overwhelming attacks on its Internet infrastructure in what some claim was the world's first act of cyber warfare. It is widely believed that Russian hackers and political activists of the Nashi variety (a pro-Putin political youth movement in Russia) were responsible for these attacks (in all likelihood with the collusion of the Kremlin). This event had a ripple effect—first within North Atlantic Treaty Organization (NATO) but the waves soon lapped at the doors of both Congress and the Pentagon.

The attacks on Estonia were followed by a now-notorious incident identified in November 2008 when, as a senior Pentagon official characterized it, a "foreign intelligence agency," succeeded in planting malware (transmitted via an infected Universal Serial Bus [USB] memory stick) on a DoD laptop in Iraq. Within a short time, the malware had spread across much of NIPRNET (Non-classified Internet Protocol Router Network), the military's unclassified network. The U.S. military works on the very sensible principle that there is much in its communications that it is happy for the world to look at.

Unfortunately for the Pentagon, somebody in the armed forces also infected SIPRNET (Secret Internet Protocol Router Network) with the virus. SIPRNET is the classified network that is kept offline (i.e., it is never connected to the Web to ensure its security from Internet-borne attacks).

In response, the United States launched an operation under the code name "Buckshot Yankee." Buckshot Yankee bolstered the argument for the creation of USCYBERCOM (the U.S. Cyber Command, an armed forces sub-unified command subordinate to the U.S. Strategic Command) and gave the National Security Agency, the developer of Buckshot Yankee, a platform from which it could press home its case. Within two years of the DoD networks' being compromised, Robert Gates, the then–Secretary of Defense, announced the formation of U.S. Cyber Command and the confirmation of a fifth military domain—cyber—to complement land, sea, air, and space. It is the first-ever manmade military domain.

NEW MILITARY COMMAND—CYBER

This was a landmark development. However one interprets it, by establishing the new command, the U.S. government was asserting that the Internet was an actual or potential vector or theater of war. In fact, by this stage, the United States and Israel had already released a series of damaging viruses aimed primarily at hindering Iran's nuclear development program, at least one of which was clearly designed to disrupt physical infrastructure. Had Iran penetrated a U.S. nuclear facility with a virus, I think we can be confident that Washington would have designated this as an act of war. In that respect, U.S. Cyber Command and the family of viruses clustered around Stuxnet, which attacked Iranian nuclear enrichment facilities, were the starting pistol for a cyber arms race (although several major countries, including Russia and China, were already developing their capabilities). Russia had been calling for discussions on cyber arms control since 1998, partly motivated by a recognition that the United States was likely to remain the premier power in terms of offensive capability.

More than 800 titles dealing with cyber warfare are available on Amazon.com. The subject may not be widely understood, but it is certainly inspiring many to put pen to paper in an effort to explain what it is and what its implications might be. Notwithstanding this intellectual effort, the issues surrounding cyber warfare remain vigorously contested among the small elite that debates them both in diplomatic fora and the more closed environment of national cyber security industries.

There are two extremes with regard to cyber warfare. First is the belief that we are already threatened by the possibility of a major assault designed to undermine the functioning of our networked computer systems. Known as "Cybergeddon" or the "Digital Pearl Harbor," it envisages the sky falling on our heads (or at the very least airplanes falling

out of the sky). The thesis proposes that our social and economic infrastructures have become so dependent on computer networks that a series of secretly introduced malware could cause havoc. Probably the best known description of this can be found in *Cyber War*[1] by Richard A. Clarke, the counterterrorism guru who has served four presidents, and Robert K. Knake:

> You look at your watch. It's now 8:15 pm. Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed in New York, Oakland, Washington, and Los Angeles. Freight trains have derailed outside major junctions and marshaling yards on four major railroads. Aircraft are literally falling out of the sky as a result of midair collisions across the country. Pipelines carrying natural gas to the Northeast have exploded, leaving millions in the cold. The financial system has also frozen solid because of terabytes of information at data centers being wiped out . . .

You get the Cassandra-esque picture.

An opposing school of thought holds that the threat of cyber warfare has been systematically exaggerated and that the nightmare visions of Richard Clarke or other "significant events," as they are also known, exist in dreams alone. These critics fall into two distinct groups. Cyber security observers, such as Bruce Schneier or Amrit Williams, have argued that sowing of FUD (Fear, Uncertainty and Doubt) by consultants like Richard Clarke is designed to bolster the fortunes of the burgeoning cyber security industry while also justifying expensive investment in high-tech weaponry by the military. Thomas Rid,[2] a reader in war studies at King's College, London, has a rather different perspective. His principal argument is that events that have been habitually characterized as cyber warfare are, in fact, nothing of a kind. Most are quotidian acts of espionage, a profession that has, of course, benefited hugely from some of its practitioners' ability to hack computer systems (although one sometimes wonders whether even the most powerful agencies have the ability to crunch all the data that they routinely pilfer). Rid sees a striking absence of physical violence in the type of attacks that are conducted in the cyber domain, suggesting that this type of attack is preferable to conventional forms of warfare in which physical violence plays a predominant role.

Any discussion about the Internet generates the widest range of opinions and, as a general rule, the less understood the subject, the more violent in tone and cacophonous the debate. Thomas Rid is certainly correct in one of his central arguments that we need a clear definition of exactly what we mean when we speak about the militarization of the Web. This is especially true with regard to the definition of a "cyber weapon" (even the DoD has no consensus on this issue). Cyber warfare constitutes perhaps the most ill-defined of discussions related to the rapid spread of networked computer systems, which have so revolutionized social, economic, and political practice.

By contrast, the debate around the nuclear deterrent, say, is quite simple. Traditionally, the development of a nuclear arsenal requires the financial and scientific resources that only a state can provide. Monitoring who already has nuclear weapons and who is seeking to develop them has been relatively straightforward. True, in recent years the Nuclear Proliferation Treaty has been slowly unraveling (sometimes with the approval of its signatories, sometimes without), nonetheless, nuclear security remains largely an issue that is the conventional concern of state actors (while acknowledging that trafficking in fissile material is also a serious matter).

INTERNET CONTROL, UNHINDERED ACCESS, AND CYBER WARFARE

This logic of deterrence does not apply to cyber security and cyber warfare—although undoubtedly in the past decade states have woken up to the fact that the Internet is far too important a tool to be left in the hands of mere citizens. Quite a few of those citizens perceive the new, more intrusive approach of the state to be a violation of their rights and the principles of the Internet and they are determined not just to express their opposition but to do something (Anonymous[3] provides a good example). A palpable tension exists between Internet activists and various interest groups on the one hand and the cyber security industry that includes state law enforcement, intelligence services, and the military on the other. Perhaps yet more ominous is the tension that exists between states with regard to the Internet as a military domain and control of networks within state boundaries.

Security strategies for the Internet impinge very quickly upon other cyber-associated issues, including freedom of speech, so-called net neutrality (which proclaims that lines carrying the Internet to users should be free of commercial interests and sponsorship), intellectual property rights, data retention, or the ability to remain anonymous on the Web. Some of these issues are discussed below.

Trying to ascertain where these issues intersect and what the implications are is one of several problems involved in most discussions about cyber warfare. But perhaps the overriding difficulty is the question of definition. What is cyber warfare? Does it exist? And how dangerous is it?

The U.S. Cyber Command (which was created to "patrol" the new domain) has two primary aims.[4] The first is relatively straightforward: "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks." (The Command is responsible for making sure that no one gains unauthorized access to U.S. military networks.)

This is admirably clear. The Pentagon has a responsibility to defend its own systems and to prevent a repeat of the SIPRNET intrusion of 2008. As important as what this includes is what it omits: the Pentagon does not take the primary role in defending the so-called Critical National Infrastructure (CNI)—by which is meant the backbone of telecoms, transport, utilities, food distribution, and the financial system.

The second part of Cyber Command's mission is more problematic. USCYBERCOM is obliged to: "prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." This vaguest of statements boils down to the U.S. military's perceived right or duty (depending on your perspective) to do anything on the Internet in furtherance of its military aims if so requested by the White House and Congress. This hinders rather than helps the task of defining what cyber warfare is or is not. And, it gives rise to the suspicion that the United States is engaged in unilateral ramping up of its cyber *offensive* capability.

It's worth mentioning here that the Department of Homeland Security (DHS) is currently responsible for protecting U.S. (nonmilitary) infrastructure against cyber attacks. Nonetheless, the debate on the issue of responsibility is by no means resolved (the Federal Bureau of Investigation [FBI], the Central Intelligence Agency [CIA], the National Security Agency [NSA], the Secret Service, and the State Department all have their say in this rather cacophonous debate). It is, however, expected that the Executive Order currently under discussion (to replace the failed legislative package) will afford the president sweeping cyber security powers while maintaining the DHS as the "official" guardian of civilian infrastructure.

CYBER CRIME

Here, let's pause to establish some basic points about malfeasance on the Web. By malfeasance we mean unauthorized access to computers anywhere in the world (although even this is a contested definition). It is helpful to break this down into four areas: cyber crime, so-called hacktivism, espionage (commercial, military, and political), and warfare.

Being a victim of cyber crime is extremely unpleasant and, in some cases of identity theft, can be quite devastating. But the great majority of everyday cyber crime that concentrates on credit and debit card fraud has now settled at a level that is less threatening—more on par with street crime.

Cyber crime has been reduced because: first, banks and credit card issuers have become more serious about security (although the opportunities for credit card fraud in the United States remain significant) and, second, serious cyber criminals have graduated into more lucrative sectors of the business.

The fastest growing sector of cyber crime is moving into the area of cyber industrial espionage. Over the past two years, law enforcement agencies worldwide along with private cyber security companies have observed a steady increase in the incidence of attacks on corporations and companies that are specifically tailored to the victim.

One of four motives is usually behind these attacks. The first is simple pecuniary gain. A common example is what is known as "data kidnapping" where a criminal hacker gains access to a company's systems and seeks out, for example, its sales database. The criminal then places an encrypted password on that data and demands a sum of money from management as the price for unlocking the database.

The second is classic industrial espionage: a competitor hires a hacker to penetrate a rival's systems so that it can access, say, its product development data to gain an unfair advantage in the market. The United States and Western Europe believe that Russia's and China's commercial espionage activity is so pervasive that in its annual report to Congress, the Office of the National Counter-Intelligence Executive noted that cyber economic espionage is a "pervasive threat" to the United States and has surpassed traditional forms of spying. Departing from diplomatic tradition of not naming countries, the report also stated that "(...) the governments of China and Russia will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyber space."[5]

This summer, Jonathan Evans, the director of MI5, Britain's domestic intelligence agency, stepped out of the shadows to warn that the level of attacks was now "astonishing."[6] According to government sources, two years ago, Britain was recording four targeted attacks per day against British companies and institutions; however, this year they were registering 500 every single hour.

A third, more recent risk stems from the ire of the "hacktivists," groups like Anonymous that target companies or institutions that they perceive to have acted politically in a manner unacceptable to Anonymous. The object of intense investigation by the FBI and other police forces, Anonymous has proved to be very effective hackers, embarrassing companies such as Sony, the consultancy firm, Stratfor, the FBI itself, and a number of cyber security companies whose very job it is to advise others on how not to become victims of Anonymous. The activities of groups like Anonymous have real implications for national security as well since they regard many of the regulatory, law enforcement, and intelligence operations on the Web as intrinsically inimical.

And, finally, in a world where extensive privatization has resulted in government outsourcing much of its security infrastructure and in which information is an increasingly valuable asset, both state and non-state actors in the cyber sphere are interested in discovering the secrets of companies working in the security, information technology, and financial sectors.

CONNECTED AND INTERCONNECTED—THE ACHILLES' HEEL

Everyone's life would be easier if the established categories of cyber crime, cyber industrial espionage, and cyber warfare remained separate. This, however, is impossible. The very genius of the Internet lies in its connectedness. This is also its Achilles' heel.

In part because of their novelty and in part because everything on the Web soon becomes tangled, we have to live with categories that overlap to such a degree that they sometimes mutate into new categories. It is quite possible, for example, for a workaday cyber criminal, who spends most of his time engaged in the "high-volume, low-impact" activity of buying, selling, or using stolen credit cards, to receive a commission to break into a major company's Web files with the express aim of obtaining specific data. His hacking skills have thus allowed him to shift into the world of commercial espionage.

Similarly, police in the United States and Western Europe have uncovered several cases of insurgent or terrorist groups, such as Al Qaeda affiliates or Tamil Tiger supporters, engaging in cyber crime to raise money. Accordingly, both the police and intelligence agencies need to monitor the activities and discussions of cyber criminals on the Internet.

The especially intimate relationship between military and intelligence in cyber space was reflected in the then-Secretary of Defense's choice to head U.S. Cyber Command, Keith Alexander. The four-star general was already head of the NSA, which plays an immensely important role in the national cyber security of the United States.

The NSA has a greater digital reach than any other organization in the world. In collaboration with the signals intelligence services of Britain, Canada, Australia, and New Zealand, it has the most powerful espionage capability. This gives the United States and the Anglophone world an advantage in all aspects of cyber security and cyber warfare. It also goes some way to explain why China and Russia appear to be hyperactive in the sphere of digital espionage—from their perspective, the combination of the NSA, Darpa, American universities, and Silicon Valley entrepreneurs ensures that the playing field is not level.

Worth highlighting here is a recent report, "The State of Broadband 2012: Achieving Digital Inclusion for All," that maintains that, as of May 2011, there were 565 million English-speaking Internet users compared with 510 Chinese-speaking users.[7] If current usage growth rates continue, Chinese will soon overtake English as the main language of the Web. This may create severe problems for intelligence services in the Anglophone world where limited investment is being made in improving and enlarging linguistic capacities (this is especially noticeable in Europe, which has instituted huge cuts in education budgets as a consequence of the current economic crisis).

VALUABLE DATA, VALUABLE ACCESS

China and Russia are also jealous of the access that American agencies have to the data of companies like Google, Facebook, and Twitter—all of which incorporated in the United States. With a court order, law enforcement or U.S. intelligence can gain access any Google or Facebook account to assist with an investigation within 24 hours of applying for it. For the same access, police officers from a friendly country like Britain would have to wait up to six months (by which time the birds have usually flown). If you are a Russian or Chinese police officer, you will never gain access through legal means.

The huge repositories of personal data held by the big information technology companies are very valuable. So, in the absence of a legal route, in 2010 and 2011, the Chinese chose to hack into Google and nine other major companies, including Adobe, producer of the pdf reader (pdf files are one of the most common routes in mounting espionage and criminal attacks).

As soon as the discovery of this hack was announced, Secretary of State Hillary Clinton made a speech in which she effectively described Google as a U.S. national security asset.[8] This is another profoundly gray area. If data is the currency of the information age, then companies like Google function as the equivalent of the Federal Reserve. One of the Gmail accounts that the Chinese hacked belonged to a human rights' activist. Google and the United States are committed to freedom of speech on the Web, but Beijing regards facilitating that right for a Chinese citizen as what would have been termed during the cold war as "an unwarranted interference into the internal affairs" of a sovereign state. This fundamental conflict (and contradiction) of interests between the United States and the European Union on the one hand and Russia and China on the other has a huge effect on the Sisyphean attempts to find common ground for establishing rules of the cyber war game.

Clinton's speech triggered a flurry of diplomatic activity focused on the key but often baffling issue of Internet governance (who actually administers the nuts and bolts of the Internet) and cyber crime. But, these initiatives never came together into a coherent narrative.

THE PROBLEM OF VIRAL ATTRIBUTION

As these efforts were under way, another event of huge significance occurred—the discovery of the Stuxnet virus. Most people suspected that either the United States and/or Israel were behind the development and insertion of this virus, which sought to disrupt the pump mechanism at Iran's uranium enrichment facilities at Natanz and other nuclear facilities. However, no definitive proof has come to light and at least one respected researcher argued that the construction of the virus suggested it was of Chinese origin (one reason why this idea did not gain much traction is that few could discern any political advantage to China of Stuxnet). The confusion highlights a very serious problem with cyber warfare—the question of attribution. The origin of an attack can never be determined with certainty; for more than a year, ignorance as to the virus's origin kept unclear the implications for the regulation of cyber space as a military domain.

After Stuxnet, researchers at the Russian antivirus laboratory, Kaspersky, discovered other related viruses, which suggests that this was not merely a one-time attack but part of a coordinated campaign.

Then, in April of this year, the White House leaked to David Sanger of the *New York Times* that the United States and Israel were behind Stuxnet (and, by extension, the other viruses in the batch that shared several characteristics).[9] It is hard to determine why the Obama administration decided to release this information, although Sanger has implied that by taking the lead with Stuxnet, the Israeli government might be less inclined to go ahead with a conventional

weapons strike on Iran. The announcement coincided with attempts by the Romney campaign to portray Obama as soft on Iran and an unreliable ally to Israel. Highlighting the American role in Stuxnet may well have been designed to counter these accusations.

Whatever the calculation, the announcement changed the environment fundamentally. Stuxnet is now widely regarded as the first shot of the starting pistol for an unregulated arms race in cyber space, although Moscow and Beijing might argue that it had already started in the 1990s. Furthermore, Stuxnet has driven a slight wedge between the U.S. government and part of the cyber security industry—the antivirus companies. Investigations into Stuxnet and its siblings, Duqu and Flame (which, unlike Stuxnet, were not designed to disrupt facilities but were conventional espionage tools), revealed that this malware had been around as far back as 2008 and that the developers had invested considerable money and time in making it undetectable to antivirus software.

FALLOUT FROM STUXNET

Until this point, the United States and the European Union had maintained a rather creditable position of and reputation for combatting malware and malicious hackers across the Web. This was in contrast to several other countries, notably Russia and China, who were mobilizing their countries' hacking capacity and, where they deemed necessary, malware for espionage activities. At the same time, North American and European private companies developed legitimate espionage and surveillance capabilities and then sold them to countries to use them against their citizens.

Since Stuxnet, however, the gloves are off. State agencies and private security companies have proliferated in Europe and America; they appear to be developing malware for the purposes of law enforcement, espionage, or warfare. Some of these private companies are also developing "strategic and tactical measures for combating adversaries."

In the meantime, China and Russia have continued to impose controls over Internet usage within their borders. In China, the government is actively trying to control the content that Chinese Internet users can access, while in Russia, the government is further deploying surveillance mechanisms on the "runet," as the Web is known colloquially.

Given the digital cacophony in cyber space, it might appear desirable to introduce some form of regulation or, at the very least, some generally agreed-on principles about what states should or should not be doing in cyber space.

Unquestionably, the three most important powers in cyber space are the United States, Russia, and China (with Israel, France, Germany, and Britain forming the second tier). It is perhaps comforting that these three nations have been trying to make progress in bilateral talks in the last few years. However, what was quickly evident is that their positions are incompatible. Through various regional institutions, Russia has been advancing its line that any agreement on Internet regulation must include a provision to exclude "action in cyber space in order to undermine the political, economic, and social system of another state, the psychological treatment of its population, destabilizing society," as its proposed Convention on International Information Security states.

The West is pushing its Budapest Convention on Cyber Crime, which argues that states should permit foreign law enforcement officers to penetrate networks in foreign jurisdictions. This is anathema to Moscow and Beijing. Russia and China may be prepared to come to an agreement about the use of cyber weaponry but only at the price of the United States agreeing to recognize that they can wield complete sovereignty over the Web within their national boundaries and in territories where they have jurisdiction.

UPCOMING INTERNET SOVEREIGNTY SUMMIT

In the wake of the failure of bilaterals, Russia and China have now moved discussions to the United Nations and the body responsible for telecommunications regulation, the International Telecommunications Union (ITU). In December 2012, it is scheduled to hold a summit meeting in Dubai in what promises to be the start of a marathon diplomatic process. Traditionally, the ITU has operated by consensus—it is one of the least fractious UN-sponsored bodies. For Russia and China, the importance of the ITU meeting lies in the issue of Internet governance—they want enshrined in international law the right to control and monitor everything that goes in, out, and around the Internet in their countries.

But, the meeting in Dubai threatens the consensus. The United States enjoys the support of most of Europe, but it finds itself isolated in some significant cyber powers and key emerging markets, notably India and Brazil.

For the moment, controlled peace exists in cyber space. But, if the logic of the last two years continues, the next five years are likely to witness two things. First, the global Internet will fracture steadily into a series of giant intranets. Iran has already indicated that it intends to cut itself off from the Internet—in part to protect itself from further cyber attacks and in part to seal itself off from "cultural contamination."

Second, states around the world will continue to develop cyber offensive weaponry on the reasonable assumption that potential enemies will be doing the same. We are currently locked into an escalating spiral of weapons' development. Whether this will have the catastrophic consequences feared by analysts like Richard C. Clarke or whether, as Thomas Rid argues, the shifting of espionage over to cyber will actually relax tensions and reduce the possibility of great power conflict is an open question.

Notes

1. Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Harper Collins, 2010).
2. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, vol. 35, no. 1 (2012): 5–32.
3. Anonymous is a loose and leaderless coalition of operations. The group takes on different political and societal issues, with the more radical elements using tools such as DDoS attacks, Web defacements, malware, and network breaches against targets.
4. See http://www.stratcom.mil/factsheets/cyber_command.
5. U.S. Office of the Director of National Intelligence, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, November 2011.
6. See http://www.bbc.co.uk/news/uk-18586681.
7. "The State of Broadband 2012: Achieving Digital Inclusion for All," a report by the Broadband Commission, September 2012, ITU and UNESCO, http://www.broadbandcommission.org/Documents/bb-annualreport2012.pdf.
8. *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html.
9. *New York Times*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.