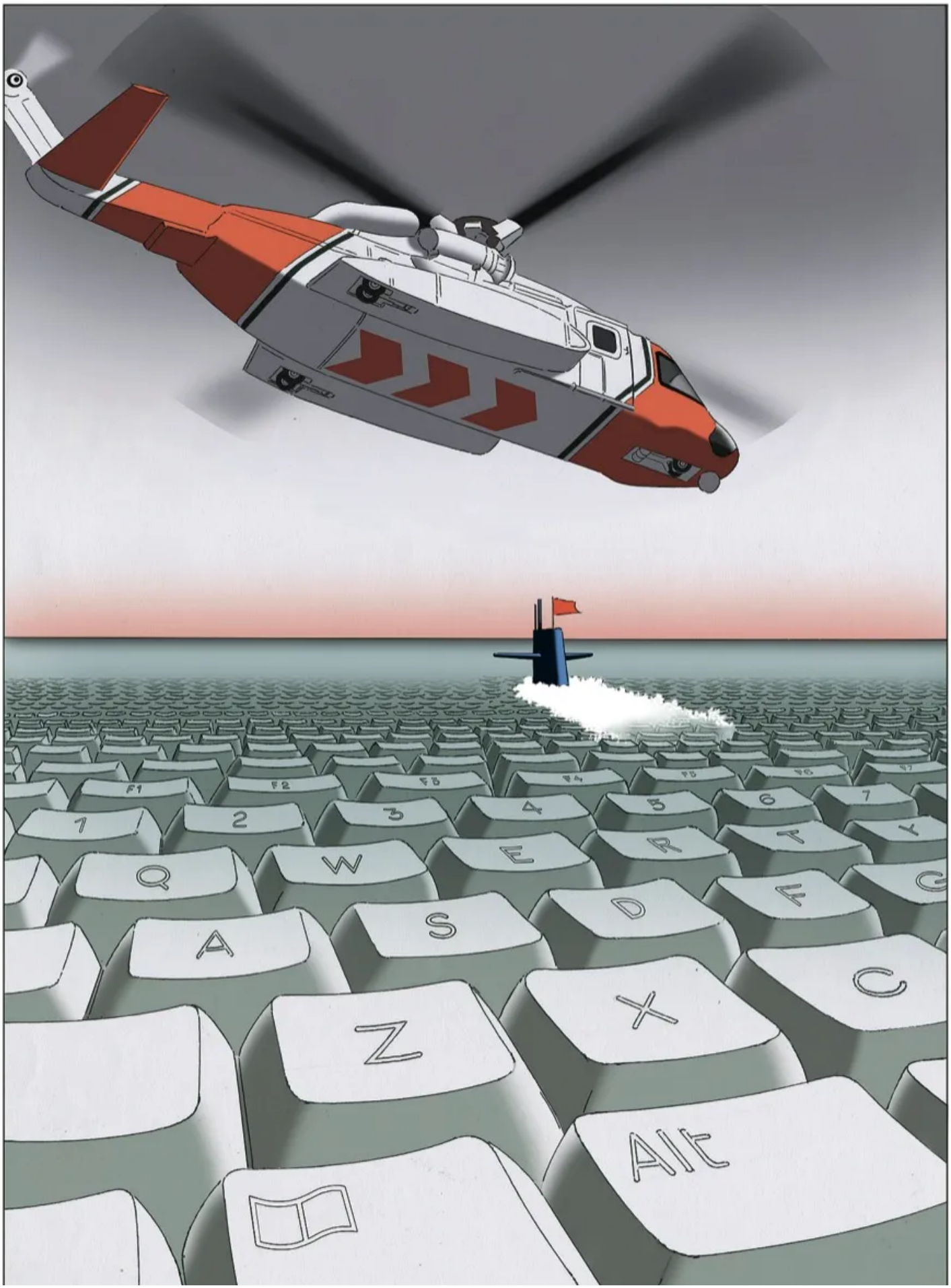
ANNALS OF NATIONAL SECURITY

THE ONLINE THREAT

By Seymour M. Hersh

October 25, 2010


F1
F2
1
2
3
4
5
6
7
Q
W
E
R
T
Y
A
S
D
F
G
Z
X
C
Alt

Some experts say that the real danger lies in confusing cyber espionage with cyber war. Illustration by Guy Billout

On April 1, 2001, an American EP-3E Aries II reconnaissance plane on an eavesdropping mission collided with a Chinese interceptor jet over the South China Sea, triggering the first international crisis of George W. Bush's Administration. The Chinese jet crashed, and its pilot was killed, but the pilot of the American aircraft, Navy Lieutenant Shane Osborn, managed to make an emergency landing at a Chinese F-8 fighter base on Hainan Island, fifteen miles from the mainland. Osborn later published a memoir, in which he described the "incessant jackhammer vibration" as the plane fell eight thousand feet in thirty seconds, before he regained control.

The plane carried twenty-four officers and enlisted men and women attached to the Naval Security Group Command, a field component of the National Security Agency. They were repatriated after eleven days; the plane stayed behind. The Pentagon told the press that the crew had followed its protocol, which called for the use of a fire axe, and even hot coffee, to disable the plane's equipment and software. These included an operating system created and controlled by the N.S.A., and the drivers needed to monitor encrypted Chinese radar, voice, and electronic communications. It was more than two years before the Navy acknowledged that things had not gone so well. "Compromise by the People's Republic of China of undestroyed classified material . . . is highly probable and cannot be ruled out," a Navy report issued in September, 2003, said.

The loss was even more devastating than the 2003 report suggested, and its dimensions have still not been fully revealed. Retired Rear Admiral Eric McVadon, who flew patrols off the coast of Russia and served as a defense attaché in Beijing, told me that the radio reports from the aircraft indicated that essential electronic gear had been dealt with. He said that the crew of the

EP-3E managed to erase the hard drive—"zeroed it out"—but did not destroy the hardware, which left data retrievable: "No one took a hammer." Worse, the electronics had recently been upgraded. "Some might think it would not turn out as badly as it did, but I sat in some meetings about the intelligence cost," McVadon said. "It was grim."

The Navy's experts didn't believe that China was capable of reverse-engineering the plane's N.S.A.-supplied operating system, estimated at between thirty and fifty million lines of computer code, according to a former senior intelligence official. Mastering it would give China a road map for decrypting the Navy's classified intelligence and operational data. "If the operating system was controlling what you'd expect on an intelligence aircraft, it would have a bunch of drivers to capture radar and telemetry," Whitfield Diffie, a pioneer in the field of encryption, said. "The plane was configured for what it wants to snoop, and the Chinese would want to know what we wanted to know about them—what we could intercept and they could not." And over the next few years the U.S. intelligence community began to "read the tells" that China had access to sensitive traffic.

The U.S. realized the extent of its exposure only in late 2008. A few weeks after Barack Obama's election, the Chinese began flooding a group of communications links known to be monitored by the N.S.A. with a barrage of intercepts, two Bush Administration national-security officials and the former senior intelligence official told me. The intercepts included details of planned American naval movements. The Chinese were apparently showing the U.S. their hand. ("The N.S.A. would ask, 'Can the Chinese be that good?' " the former official told me. "My response was that they only invented gunpowder in the tenth century and built the bomb in 1965. I'd say, 'Can you read Chinese?' We don't even know the Chinese pictograph for 'Happy hour.' ")

Why would the Chinese reveal that they had access to American

communications? One of the Bush national-security officials told me that some of the aides then working for Vice-President Dick Cheney believed—or wanted to believe—that the barrage was meant as a welcome to President Obama. It is also possible that the Chinese simply made a mistake, given the difficulty of operating surgically in the cyber world.

Admiral Timothy J. Keating, who was then the head of the Pacific Command, convened a series of frantic meetings in Hawaii, according to a former C.I.A. official. In early 2009, Keating brought the issue to the new Obama Administration. If China had reverse-engineered the EP-3E's operating system, all such systems in the Navy would have to be replaced, at a cost of hundreds of millions of dollars. After much discussion, several current and former officials said, this was done. (The Navy did not respond to a request for comment on the incident.)

Admiral McVadon said that the loss prompted some black humor, with one Navy program officer quoted as saying, "This is one hell of a way to go about getting a new operating system."

The EP-3E debacle fuelled a longstanding debate within the military and in the Obama Administration. Many military leaders view the Chinese penetration as a warning about present and future vulnerabilities—about the possibility that China, or some other nation, could use its expanding cyber skills to attack America's civilian infrastructure and military complex. On the other side are those who argue for a civilian response to the threat, focussed on a wider use of encryption. They fear that an overreliance on the military will have adverse consequences for privacy and civil liberties.

In May, after years of planning, the U.S. Cyber Command was officially activated, and took operational control of disparate cyber-security and attack units that had been scattered among the four military services. Its commander,

Army General Keith Alexander, a career intelligence officer, has made it clear that he wants more access to e-mail, social networks, and the Internet to protect America and fight in what he sees as a new warfare domain—cyberspace. In the next few months, President Obama, who has publicly pledged that his Administration will protect openness and privacy on the Internet, will have to make choices that will have enormous consequences for the future of an ever-growing maze of new communication techniques: Will America's networks be entrusted to civilians or to the military? Will cyber security be treated as a kind of war?

Even as the full story of China's EP-3E coup remained hidden, "cyber war" was emerging as one of the nation's most widely publicized national-security concerns. Early this year, Richard Clarke, a former White House national-security aide who warned about the threat from Al Qaeda before the September 11th attacks, published "Cyber War," an edgy account of America's vulnerability to hackers, both state-sponsored and individual, especially from China. "Since the late 1990s, China has systematically done all the things a nation would do if it contemplated having an offensive cyber war capability," Clarke wrote. He forecast a world in which China might unleash havoc:

> 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. . . . Aircraft are literally falling out of the sky as a result of midair collisions across the country. . . . Several thousand Americans have already died.

Retired Vice-Admiral J. Michael McConnell, Bush's second director of National Intelligence, has issued similar warnings. "The United States is fighting a cyber war today, and we are losing," McConnell wrote earlier this year in the Washington *Post*. "Our cyber-defenses are woefully lacking." In February, in testimony before the Senate Commerce, Science, and

Transportation Committee, he said, "As a consequence of not mitigating the risk, we're going to have a catastrophic event."

A great deal of money is at stake. Cyber security is a major growth industry, and warnings from Clarke, McConnell, and others have helped to create what has become a military-cyber complex. The federal government currently spends between six and seven billion dollars annually for unclassified cyber-security work, and, it is estimated, an equal amount on the classified portion. In July, the Washington *Post* published a critical assessment of the unchecked growth of government intelligence agencies and private contractors. Benjamin Powell, who served as general counsel for three directors of the Office of National Intelligence, was quoted as saying of the cyber-security sector, "Sometimes there was an unfortunate attitude of bring your knives, your guns, your fists, and be fully prepared to defend your turf. . . . Because it's funded, it's hot and it's sexy."

Clarke is the chairman of Good Harbor Consulting, a strategic-planning firm that advises governments and companies on cyber security and other issues. (He says that more than ninety per cent of his company's revenue comes from non-cyber-related work.) McConnell is now an executive vice-president of Booz Allen Hamilton, a major defense contractor. Two months after McConnell testified before the Senate, Booz Allen Hamilton landed a thirty-four-million-dollar cyber contract. It included fourteen million dollars to build a bunker for the Pentagon's new Cyber Command.

American intelligence and security officials for the most part agree that the Chinese military, or, for that matter, an independent hacker, is theoretically capable of creating a degree of chaos inside America. But I was told by military, technical, and intelligence experts that these fears have been exaggerated, and are based on a fundamental confusion between cyber espionage and cyber war. Cyber espionage is the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence. Cyber war involves the penetration of foreign networks for the purpose of disrupting or dismantling those networks, and making them inoperable. (Some of those I spoke to made the point that China had demonstrated its mastery of cyber espionage in the EP-3E incident, but it did not make overt use of it to wage cyber war.) Blurring the distinction between cyber war and cyber espionage has been profitable for defense contractors—and dispiriting for privacy advocates.

Clarke's book, with its alarming vignettes, was praised by many reviewers. But it received much harsher treatment from writers in the technical press, who pointed out factual errors and faulty assumptions. For example, Clarke attributed a severe power outage in Brazil to a hacker; the evidence pointed to sooty insulators.

The most common cyber-war scare scenarios involve America's electrical grid. Even the most vigorous privacy advocate would not dispute the need to improve the safety of the power infrastructure, but there is no documented case of an electrical shutdown forced by a cyber attack. And the cartoonish view that a hacker pressing a button could cause the lights to go out across the country is simply wrong. There is no national power grid in the United States. There are more than a hundred publicly and privately owned power companies that operate their own lines, with separate computer systems and separate security arrangements. The companies have formed many regional grids, which means that an electrical supplier that found itself under cyber attack would be able to

avail itself of power from nearby systems. Decentralization, which alarms security experts like Clarke and many in the military, can also protect networks.

In July, there were reports that a computer worm, known as Stuxnet, had infected thousands of computers worldwide. Victims, most of whom were unharmed, were able to overcome the attacks, although it sometimes took hours or days to even notice them. Some of the computers were inside the Bushehr nuclear-energy plant, in Iran, and this led to speculation that Israel or the United States might have developed the virus. A Pentagon adviser on information warfare told me that it could have been an attempted "semantic attack," in which the virus or worm is designed to fool its victim into thinking that its computer systems are functioning properly, when in fact they are not, and may not have been for some time. (This month, Microsoft, whose Windows operating systems were the main target of Stuxnet, completed a lengthy security fix, or patch.)

If Stuxnet was aimed specifically at Bushehr, it exhibited one of the weaknesses of cyber attacks: they are difficult to target and also to contain. India and China were both hit harder than Iran, and the virus could easily have spread in a different direction, and hit Israel itself. Again, the very openness of the Internet serves as a deterrent against the use of cyber weapons.

Bruce Schneier, a computer scientist who publishes a widely read blog on cyber security, told me that he didn't know whether Stuxnet posed a new threat. "There's certainly no actual evidence that the worm is targeted against Iran or anybody," he said in an e-mail. "On the other hand, it's very well designed and well written." The real hazard of Stuxnet, he added, might be that it was "great for those who want to believe cyber war is here. It is going to be harder than ever to hold off the military."

A defense contractor who is regarded as one of America's most knowledgeable

experts on Chinese military and cyber capabilities took exception to the phrase "cyber war." "Yes, the Chinese would love to stick it to us," the contractor told me. "They would love to transfer economic and business innovation from West to East. But cyber espionage is not cyber war." He added, "People have been sloppy in their language. McConnell and Clarke have been pushing cyber war, but their evidentiary basis is weak."

James Lewis, a senior fellow at the Center for Strategic and International Studies, who worked for the Departments of State and Commerce in the Clinton Administration, has written extensively on the huge economic costs due to cyber espionage from China and other countries, like Russia, whose hackers are closely linked to organized crime. Lewis, too, made a distinction between this and cyber war: "Current Chinese officials have told me that we're not going to attack Wall Street, because we basically own it"—a reference to China's holdings of nearly a trillion dollars in American securities—"and a cyber-war attack would do as much economic harm to us as to you."

Nonetheless, China "is in full economic attack" inside the United States, Lewis says. "Some of it is economic espionage that we know and understand. Some of it is like the Wild West. Everybody is pirating from everybody else. The U.S.'s problem is what to do about it. I believe we have to begin by thinking about it"—the Chinese cyber threat—"as a trade issue that we have not dealt with."

The bureaucratic battle between the military and civilian agencies over cyber security—and the budget that comes with it—has made threat assessments more problematic. General Alexander, the head of Cyber Command, is also the director of the N.S.A., a double role that has caused some apprehension, particularly on the part of privacy advocates and civil libertarians. (The N.S.A. is formally part of the Department of Defense.) One of Alexander's first goals was to make sure that the military would take the lead role in cyber security and in determining the future shape of computer

networks. (A Department of Defense spokesman, in response to a request to comment on this story, said that the department "continues to adhere to all laws, policies, directives, or regulations regarding cyberspace. The Department of Defense maintains strong commitments to protecting civil liberties and privacy.")

The Department of Homeland Security has nominal responsibility for the safety of America's civilian and private infrastructure, but the military leadership believes that the D.H.S. does not have the resources to protect the electrical grids and other networks. (The department intends to hire a thousand more cyber-security staff members over the next three years.) This dispute became public when, in March, 2009, Rodney Beckstrom, the director of the D.H.S.'s National Cybersecurity Center, abruptly resigned. In a letter to Secretary Janet Napolitano, Beckstrom warned that the N.S.A. was effectively controlling her department's cyber operations: "While acknowledging the critical importance of N.S.A. to our intelligence efforts . . . the threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization." Beckstrom added that he had argued for civilian control of cyber security, "which interfaces with, but is not controlled by, the N.S.A."

General Alexander has done little to reassure critics about the N.S.A.'s growing role. In the public portion of his confirmation hearing, in April, before the Senate Armed Services Committee, he complained of a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."

Alexander later addressed a controversial area: when to use conventional armed forces to respond to, or even preëmpt, a network attack. He told the senators that one problem for Cyber Command would be to formulate a response based

on nothing more than a rough judgment about a hacker's intent. "What's his game plan? Does he have one?" he said. "These are tough issues, especially when attribution and neutrality are brought in, and when trying to figure out what's come in." At this point, he said, he did not have "the authority . . . to reach out into a neutral country and do an attack. And therein lies the complication. . . . What do you do to take that second step?"

Making the same argument, William J. Lynn III, the Deputy Secretary of Defense, published an essay this fall in *Foreign Affairs* in which he wrote of applying the N.S.A.'s "defense capabilities beyond the '.gov' domain," and asserted, "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare." This definition raises questions about where the battlefield begins and where it ends. If the military is operating in "cyberspace," does that include civilian computers in American homes?

Lynn also alluded to a previously classified incident, in 2008, in which some N.S.A. unit commanders, facing penetration of their bases' secure networks, concluded that the break-in was caused by a disabling thumb drive; Lynn said that it had been corrupted by "a foreign intelligence agency." (According to press reports, the program was just as likely to be the product of hackers as that of a government.) Lynn termed it a "wakeup call" and a "turning point in U.S. cyber defense strategy." He compared the present moment to the day in 1939 when President Franklin D. Roosevelt got a letter from Albert Einstein about the possibility of atomic warfare.

But Lynn didn't mention one key element in the commanders' response: they ordered all ports on the computers on their bases to be sealed with liquid cement. Such a demand would be a tough sell in the civilian realm. (And a Pentagon adviser suggested that many military computer operators had simply ignored the order.)

A senior official in the Department of Homeland Security told me, "Every time the N.S.A. gets involved in domestic security, there's a hue and cry from people in the privacy world." He said, though, that coöperation between the military and civilians had increased. (The Department of Homeland Security recently signed a memorandum with the Pentagon that gives the military authority to operate inside the United States in case of cyber attack.) "We need the N.S.A., but the question we have is how to work with them and still say and demonstrate that we are in charge in the areas for which we are responsible."

This official, like many I spoke to, portrayed the talk about cyber war as a bureaucratic effort "to raise the alarm" and garner support for an increased Defense Department role in the protection of private infrastructure. He said, "You hear about cyber war all over town. This"—he mentioned statements by Clarke and others—"is being done to mobilize a political effort. We always turn to war analogies to mobilize the people."

In theory, the fight over whether the Pentagon or civilian agencies should be in charge of cyber security should be mediated by President Obama's coördinator for cyber security, Howard Schmidt—the cyber czar. But Schmidt has done little to assert his authority. He has no independent budget control and in a crisis would be at the mercy of those with more assets, such as General Alexander. He was not the Administration's first choice for the cyber-czar job—reportedly, several people turned it down. The Pentagon adviser on

information warfare, in an e-mail that described the lack of an over-all policy and the "cyber-pillage" of intellectual property, added the sort of dismissive comment that I heard from others: "It's ironic that all this goes on under the nose of our first cyber President. . . . Maybe he should have picked a cyber czar with more than a mail-order degree." (Schmidt's bachelor's and master's degrees are from the University of Phoenix, though from one of their "ground" campuses.)

Howard Schmidt doesn't like the term "cyber war." "The key point is that cyber war benefits no one," Schmidt told me in an interview at the Old Executive Office Building. "We need to focus on that fact. When people tell me that these guys or this government is going to take down the U.S. military with information warfare I say that, if you look at the history of conflicts, there's always been the goal of intercepting the communications of combatants—whether it's cutting down telephone poles or intercepting Morse-code signalling. We have people now who have found that warning about 'cyber war' has become an unlikely career path"—an obvious reference to McConnell and Clarke. "All of a sudden, they have become experts, and they get a lot of attention. 'War' is a big word, and the media is responsible for pushing this, too. Economic espionage on the Internet has been mischaracterized by people as cyber war."

Schmidt served in Vietnam, worked as a police officer for several years on a SWAT team in Arizona, and then specialized in computer-related crimes at the F.B.I. and in the Air Force's investigative division. In 1997, he joined Microsoft, where he became chief of security, leaving after the 9/11 attacks to serve in the Bush Administration as a special adviser for cyber security. When Obama hired him, he was working as the head of security for eBay. When I asked him about the ongoing military-civilian dispute, Schmidt said, "The middle way is not to give too much authority to one group or another and to

make sure that we share information with each other."

Schmidt continued, "We have to protect our infrastructure and our way of life, for sure. We do have vulnerabilities, and we do talk about worst-case scenarios" with the Pentagon and the Department of Homeland Security. "You don't see a looming war and just wait for it to come." But, at the same time, "we have to keep our shipping lanes open, to continue to do commerce, and to freely use the Internet."

How should the power grid be protected? It does remain far too easy for a sophisticated hacker to break into American networks. In 2008, the computers of both the Obama and the McCain campaigns were hacked. Suspicion fell on Chinese hackers. People routinely open e-mails with infected attachments, allowing hackers to "enslave" their computers. Such machines, known as zombies, can be linked to create a "botnet," which can flood and effectively shut down a major system. Hackers are also capable of penetrating a major server, like Gmail. Guesses about the cost of cyber crime vary widely, but one survey, cited by President Obama in a speech in May, 2009, put the price at more than eight billion dollars in 2007 and 2008 combined. Obama added, referring to corporate cyber espionage, "It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to one trillion dollars."

One solution is mandated encryption: the government would compel both corporations and individuals to install the most up-to-date protection tools. This option, in some form, has broad support in the technology community and among privacy advocates. In contrast, military and intelligence eavesdroppers have resisted nationwide encryption since 1976, when the Diffie-Hellman key exchange (an encryption tool co-developed by Whitfield Diffie) was invented, for the most obvious of reasons: it would hinder their ability to

intercept signals. In this sense, the N.S.A.'s interests align with those of the hackers.

John Arquilla, who has taught since 1993 at the U.S. Naval Postgraduate School in Monterey, California, writes in his book "Worst Enemies," "We would all be far better off if virtually all civil, commercial, governmental, and military internet and web traffic were strongly encrypted." Instead, many of those charged with security have adopted the view that "cyberspace can be defended with virtual fortifications—basically the 'firewalls' that everyone knows about. . . . A kind of Maginot Line mentality prevails."

Arquilla added that America's intelligence agencies and law-enforcement officials have consistently resisted encryption because of fears that a serious, widespread effort to secure data would interfere with their ability to electronically monitor and track would-be criminals or international terrorists. This hasn't stopped sophisticated wrongdoers from, say, hiring hackers or encrypting files; it just leaves the public exposed, Arquilla writes. "Today drug lords still enjoy secure internet and web communications, as do many in terror networks, while most Americans don't."

Schmidt told me that he supports mandated encryption for the nation's power and electrical infrastructure, though not beyond that. But, early last year, President Obama declined to support such a mandate, in part, Schmidt said, because of the costs it would entail for corporations. In addition to the setup expenses, sophisticated encryption systems involve a reliance on security cards and on constantly changing passwords, along with increased demands on employees and a ceding of control by executives to their security teams.

General Alexander, meanwhile, has continued to press for more authority, and even for a separate Internet domain—another Maginot Line, perhaps. One morning in September, he told a group of journalists that the Cyber Command

needed what he called "a secure zone," a separate space within the Internet to shelter the military and essential industries from cyber attacks. The secure zone would be kept under tight government control. He also assured the journalists, according to the *Times*, that "we can protect civil liberties, privacy, and still do our mission." The General was more skeptical about his ability to please privacy advocates when he testified, a few hours later, before the House Armed Services Committee: "A lot of people bring up privacy and civil liberties. And then you say, 'Well, what specifically are you concerned about?' And they say, 'Well, privacy and civil liberties.' . . . Are you concerned that the anti-virus program that McAfee runs invades your privacy or civil liberties?' And the answer is 'No, no, no—but I'm worried that you would.' "

This summer, the *Wall Street Journal* reported that the N.S.A. had begun financing a secret surveillance program called Perfect Citizen to monitor attempted intrusions into the computer networks of private power companies. The program calls for the installation of government sensors in those networks to watch for unusual activity. The *Journal* noted that some companies expressed concerns about privacy, and said that what they needed instead was better guidance on what to do in case of a major cyber attack. The N.S.A. issued a rare public response, insisting that there was no "monitoring activity" involved: "We strictly adhere to both the spirit and the letter of U.S. laws and regulations."

A former N.S.A. operative I spoke to said, of Perfect Citizen, "This would put the N.S.A. into the job of being able to watch over our national communications grid. If it was all dot-gov, I would have no problem with the sensors, but what if the private companies rely on Gmail or att.net to communicate? This could put the N.S.A. into every service provider in the country."

The N.S.A. has its own hackers. Many of them are based at a secret annex near Thurgood Marshall International Airport, outside Baltimore. (The airport used to be called Friendship Airport, and the annex is known to insiders as the FANX, for "Friendship annex.") There teams of attackers seek to penetrate the communications of both friendly and unfriendly governments, and teams of defenders monitor penetrations and attempted penetrations of U.S. systems. The former N.S.A. operative, who served as a senior watch officer at a major covert installation, told me that the N.S.A. obtained invaluable on-the-job training in cyber espionage during the attack on Iraq in 1991. Its techniques were perfected during the struggle in Kosovo in 1999 and, later, against Al Qaeda in Iraq. "Whatever the Chinese can do to us, we can do better," the technician said. "Our offensive cyber capabilities are far more advanced."

Nonetheless, Marc Rotenberg, the president of the Electronic Privacy Information Center and a leading privacy advocate, argues that the N.S.A. is simply not competent enough to take a leadership role in cyber security. "Let's put the issue of privacy of communications aside," Rotenberg, a former Senate aide who has testified often before Congress on encryption policy and consumer protection, said. "The question is: Do you want an agency that spies with mixed success to be responsible for securing the nation's security? If you do, that's crazy."

Nearly two decades ago, the Clinton Administration, under pressure from the N.S.A., said that it would permit encryption-equipped computers to be

exported only if their American manufacturers agreed to install a government-approved chip, known as the Clipper Chip, in each one. It was subsequently revealed that the Clipper Chip would enable law-enforcement officials to have access to data in the computers. The ensuing privacy row embarrassed Clinton, and the encryption-equipped computers were permitted to be exported without the chip, in what amounted to a rebuke to the N.S.A.

That history may be repeating itself. The Obama Administration is now planning to seek broad new legislation that would enable national-security and law-enforcement officials to police online communications. The legislation, similar to that sought two decades ago in the Clipper Chip debate, would require manufacturers of equipment such as the BlackBerry, and all domestic and foreign purveyors of communications, such as Skype, to develop technology that would allow the federal government to intercept and decode traffic.

"The lesson of Clipper is that the N.S.A. is really not good at what it does, and its desire to eavesdrop overwhelms its ability to protect, and puts at risk U.S. security," Rotenberg said. "The N.S.A. wants security, sure, but it also wants to get to capture as much as it can. Its view is you can get great security as long as you listen in." Rotenberg added, "General Alexander is not interested in communication privacy. He's not pushing for encryption. He wants to learn more about people who are on the Internet"—to get access to the original internal protocol, or I.P., addresses identifying the computers sending e-mail messages. "Alexander wants user I.D. He wants to know who you are talking to."

Rotenberg concedes that the government has a role to play in the cyber world. "We privacy guys want strong encryption for the security of America's infrastructure," he said. He also supports Howard Schmidt in his willingness to mandate encryption for the few industries whose disruption could lead to

chaos. “Howard is trying to provide a reasoned debate on an important issue.”

Whitfield Diffie, the encryption pioneer, offered a different note of skepticism in an e-mail to me: “It would be easy to write a rule mandating encryption but hard to do it in such a way as to get good results. To make encryption effective, someone has to manage and maintain the systems (the way N.S.A. does for D.O.D. and, to a lesser extent, other parts of government). I think that what is needed is more by way of standards, guidance, etc., that would make it easier for industry to implement encryption without making more trouble for itself than it saves.”

More broadly, Diffie wrote, “I am not convinced that lack of encryption is the primary problem. The problem with the Internet is that it is meant for communications among non-friends.”

What about China? Does it pose such a threat that, on its own, it justifies putting cyber security on a war footing? The U.S. has long viewed China as a strategic military threat, and as a potential adversary in the sixty-year dispute over Taiwan. Contingency plans dating back to the Cold War include calls for an American military response, led by a Navy carrier group, if a Chinese fleet sails into the Taiwan Strait. “They’ll want to stop our carriers from coming, and they will throw whatever they have in cyber war—everything but the kitchen sink—to blind us, or slow our fleet down,” Admiral McVadon, the retired defense attaché, said. “Our fear is that the Chinese may think that cyber war will work, but it may not. And that’s a danger because it”—a test of cyber warfare—“could lead to a bigger war.”

However, the prospect of a naval battle for Taiwan and its escalation into a cyber attack on America’s domestic infrastructure is remote. Jonathan Pollack, an expert on the Chinese military who teaches at the Naval War College in

Newport, Rhode Island, said, "The fact is that the Chinese are remarkably risk-averse." He went on, "Yes, there have been dustups, and the United States collects intelligence around China's border, but there is an accommodation process under way today between China and Taiwan." In June, Taiwan approved a trade agreement with China that had, as its ultimate goal, a political rapprochement. "The movement there is palpable, and, given that, somebody's got to tell me how we are going to find ourselves in a war with China," Pollack said.

Many long-standing allies of the United States have been deeply engaged in cyber espionage for decades. A retired four-star Navy admiral, who spent much of his career in signals intelligence, said that Russia, France, Israel, and Taiwan conduct the most cyber espionage against the U.S. "I've looked at the extraordinary amount of Russian and Chinese cyber activity," he told me, "and I am hard put to it to sort out how much is planning for warfare and how much is for economic purposes."

The admiral said that the U.S. Navy, worried about budget cuts, "needs an enemy, and it's settled on China," and that "using what your enemy is building to justify your budget is not a new game."

There is surprising unanimity among cyber-security experts on one issue: that the immediate cyber threat does not come from traditional terrorist groups like Al Qaeda, at least, not for the moment. "Terrorist groups are not particularly good now in attacking our computer system," John Arquilla told me. "They're not that interested in it—yet. The question is: Do vulnerabilities exist inside America? And, if they do, the terrorists eventually will exploit them." Arquilla added a disturbing thought: "The terrorists of today rely on cyberspace, and they have to be good at cyber security to protect *their* operations." As terrorist groups get better at defense, they may eventually turn to offense.

Jeffrey Carr, a Seattle-based consultant on cyber issues, looked into state and non-state cyber espionage throughout the recent conflicts in Estonia and Georgia. Carr, too, said he was skeptical that China or Russia would mount a cyber-war attack against the United States. “It’s not in their interest to hurt the country that is feeding them money,” he said. “On the other hand, it does make sense for lawless groups.” He envisaged “five- or six-year-old kids in the Middle East who are working on the Internet,” and who would “become radicalized fifteen- or sixteen-year-old hackers.” Carr is an advocate of making all Internet service providers require their customers to use verifiable registration information, as a means of helping authorities reduce cyber espionage.

Earlier this year, Carr published “Inside Cyber Warfare,” an account, in part, of his research into cyber activity around the world. But he added, “I hate the term ‘cyber war.’ ” Asked why he used “cyber warfare” in the title of his book, he responded, “I don’t like hype, but hype sells.”

Why not ignore the privacy community and put cyber security on a war footing? Granting the military more access to private Internet communications, and to the Internet itself, may seem prudent to many in these days of international terrorism and growing American tensions with the Muslim world. But there are always unintended consequences of military activity—some that may take years to unravel. Ironically, the story of the EP-3E aircraft that was downed off the coast of China provides an example. The account, as relayed to me by a fully informed retired American diplomat, begins with the contested Presidential election between Vice-President Al Gore and George W. Bush the previous November. That fall, a routine military review concluded that certain reconnaissance flights off the eastern coast of the former Soviet Union—daily Air Force and Navy sorties flying out of bases in the Aleutian Islands—were redundant, and recommended that they be cut back.

"Finally, on the eve of the 2000 election, the flights were released," the former diplomat related. "But there was nobody around with any authority to make changes, and everyone was looking for a job." The reality is that no military commander would unilaterally give up any mission. "So the system defaulted to the next target, which was China, and the surveillance flights there went from one every two weeks or so to something like one a day," the former diplomat continued. By early December, "the Chinese were acting aggressively toward our now increased reconnaissance flights, and we complained to our military about their complaints. But there was no one with political authority in Washington to respond, or explain." The Chinese would not have been told that the increase in American reconnaissance had little to do with anything other than the fact that inertia was driving day-to-day policy. There was no leadership in the Defense Department, as both Democrats and Republicans waited for the Supreme Court to decide the fate of the Presidency.

The predictable result was an increase in provocative behavior by Chinese fighter pilots who were assigned to monitor and shadow the reconnaissance flights. This evolved into a pattern of harassment in which a Chinese jet would maneuver a few dozen yards in front of the slow, plodding EP-3E, and suddenly blast on its afterburners, soaring away and leaving behind a shock wave that severely rocked the American aircraft. On April 1, 2001, the Chinese pilot miscalculated the distance between his plane and the American aircraft. It was a mistake with consequences for the American debate on cyber security that have yet to be fully reckoned. ♦

Published in the print edition of the November 1, 2010, issue.

Seymour M. Hersh wrote his first piece for The New Yorker in 1971 and has been a regular contributor to the magazine since 1993.

More: Barack Obama China Chinese Computers Department of Homeland Security Eavesdropping Encryption Foreign Policy Hackers Internet National Security Agency (N.S.A.) Privacy Stuxnet Technology U.S. Navy Viruses

READ MORE

POP MUSIC

The Tortured Poetry of Taylor Swift's New Album

"The Tortured Poets Department" has moments of tenderness. But it suffers from being too long and too familiar.

By Amanda Petrusich

THE NEW YORKER INTERVIEW

Jonathan Haidt Wants You to Take Away Your Kid's Phone

The social psychologist discusses the "great rewiring" of children's brains, why social-media companies are to blame, and how to reverse course.

By David Remnick

DEPT. OF MEDICINE

How to Die in Good Health

The average American celebrates just one healthy birthday after the age of sixty-five. Peter Attia argues that it doesn't have to be this way.

By Dhruv Khullar

INFINITE SCROLL

The Internet's New Favorite Philosopher

Byung-Chul Han, in treatises such as "The Burnout Society" and his latest, "The Crisis of Narration," diagnoses the frenetic aimlessness of the digital age.

By Kyle Chayka