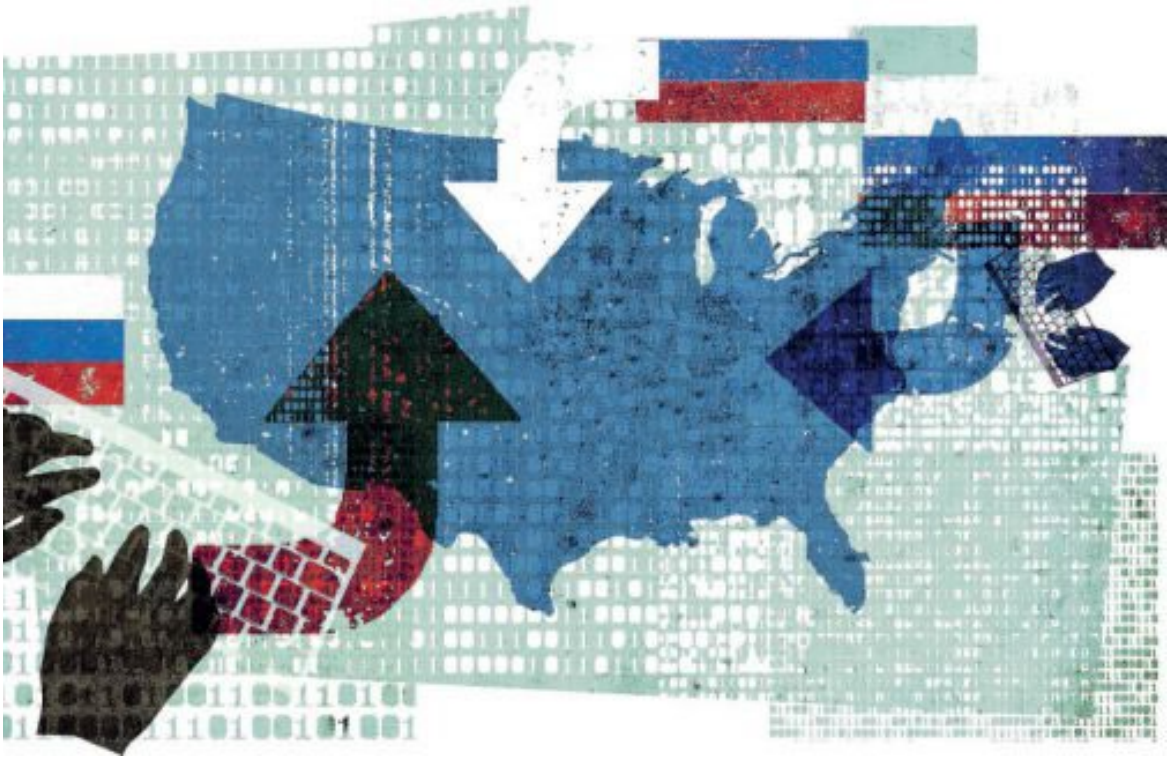
Digital Pearl Harbor:

Responses to the Growing Threat

Nicholas Rostow and Abraham Wagner



September 20, 2023

MARGIN RESEARCH

The research described in this report was sponsored by the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR00112190088. The views expressed are those of the authors and do not necessarily reflect the views of the U.S Government.

www.margin.re

Contents

Introduction

Cybersecurity has been a concern for years. Government, industry, and academia have recognized the issue but, for all intents and purposes, have failed adequately to address the most serious national security aspects of the problem. Efforts to date have focused on the technological equivalent of "low hanging fruit," not on the sophisticated and evolving capabilities being developed by potential adversaries or the prospect for a major cyber attack on the nation's most critical sectors; in effect, a digital Pearl Harbor. This metaphor captures the danger but not the way it might well be conducted.

Enough is known to take more comprehensive steps than ever before to enhance cybersecurity. One key aspect is to employ technologies to detect malicious computer code before an attack, and track those that are developing it. The second critical area is to is to achieve enhanced cyber ecosystem resilience, decreasing vulnerability to attack. This approach would make national risk management much more effective than presently is the case. The nation cannot afford to to await another Pearl Harbor or 9/11 to act to improve its cybersecurity posture.

For more than two decades, the United States has been complacent about the risk of major, large-scale or progressive cyber attack against the cyber infrastructure used by so much of contemporary society. Complacency has included tolerance of sub-optimal bureaucratic arrangements. Heightened adversary technical capabilities and worsened geopolitics require an end to that complacency. The idea that the commercial sector and private industry would solve many cyber problems has proved invalid, and even the touted "public-private partnership" likely will be insufficient to meet foreseeable challenges in the cyberlandscape. The government must take the lead.

The present cyber context requires that the nation's intelligence services monitor the development of hostile cyber warfare capabilities, creation of malicious code, and the institutions and individuals involved. Reporting cyber attacks as "incidents" after they take place is no substitute for understanding how a devastating cyber attack might be conducted and managed if not prevented. Such understanding can come only as a result of a far more disciplined approach to dealing with the threat.

This means detection of malicious computer code development so that the attack surface is made less vulnerable, and critically important systems are made more resilient. Measures are needed such as the type of expanded support infrastructure created to meet the challenge of the Soviet technology threat during the Cold War.

1. The Problem of a Devastating Cyber Attack

Technology and Geopolitics

All modern societies, whatever their political culture, now confront the potential reality of devastating attack using information and communications technologies. Some rightly draw an analogy to Pearl Harbor but the effects of a digital version of Pearl Harbor would be even more extensive, devastating, and difficult to recover from than the original.[1] The 1941 Japanese attack on Pearl Harbor involved a kinetic attack on U.S. naval ships and supporting infrastructure.

Now a determined adversary can cause substantial damage with non-kinetic cyber weapons operating remotely. They could be unleashed in scaled actions across a spectrum of possibilities targeting a variety of cyber nodes in coordinated fashion from obscured or disguised sources, making Pearl Harbor look like child's play because of the far more widespread character of the attack(s).

The Internet still operates on computer protocols developed more than 50 years ago with no thought given to security. The result is a worldwide, massive, complicated, information technology and communication superstructure resting on the security equivalent of quicksand. No matter what efforts are taken to secure an application or software, or the number of patches added for security, the system is vulnerable because the foundation itself remains vulnerable. Regular updates to all operating systems is testimony by itself to the insecurity of the worldwide web.[2]

Russian aggression against Ukraine, the increasingly unpredictable but hostile relationship between China and the United States, and the apparent likelihood that Iran will soon obtain a nuclear weapon create an uncertain geopolitical context in which major technological changes are taking place.[3] Not only may they create opportunities for the cyber equivalent of a first nuclear strike or a series of nuclear strikes, but also they may encourage hostile strategists to consider such actions as realistic. They may consider cyber disruption to be low risk because the very systems that would counter cyber attacks would be out of action as a result of such attacks. The damage would be devastating but non-kinetic.

Comparing Pearl Harbor to A Digital Attack

It is important to think about what is actually meant by a digital Pearl Harbor. "Pearl Harbor" is a metaphor for devastating surprise attack. It was intended as a knock-out blow, in essence a counterforce attack against the U.S. capacity for naval warfare in the Pacific.[4] In the nuclear context, such an attack would be called "preemptive." The Japanese may have believed that the attack would sap American morale and willingness to fight, along with crippling the U.S. capability to engage in naval warfare at the time.

Despite significant civilian casualties, it did not achieve this goal. A digital Pearl Harbor, on the other hand, would substantially reduce the U.S. ability to project military power or engage in major conventional war to the extent the U.S. military forces depend on the Internet to operate. Because the Defense Department and military services rely on civilian systems and commercial software to communicate and generate and deploy forces, an attack on critical "civilian" sectors almost certainly would have an impact on how the United States could respond militarily and in other ways.

In the nuclear context, a major concern has been the foreseeable damage to, and protection of, the economy and supporting infrastructure. This focus has been a key element of the nation's nuclear policy and targeting for many years.[5] The concept of a digital Pearl Harbor that primarily targets this civilian infrastructure also should be central to American analysis and policy.

The Attack Surface and Response

The U.S., cyber attack surface—the set of points that are susceptible to attack—is gigantic. Digital systems on which almost all sectors of society now depend are connected to networks that are highly vulnerable to attacks ranging from hacks to ransomware to devastating cyberattacks. Attackers include criminal enterprises, hostile foreign actors, and terrorists. Everything connected to information technologies that makes a modern society function is at risk. Just as the vulnerabilities run the gamut, so too attacks cover a spectrum of means.

Unlike kinetic warfare and nuclear arracks, cyberattacks can be scaled, and can range from lower level espionage to major attacks which cripple one or major critical sectors. Financial services, utilities, energy, distribution mechanisms, healthcare, transportation, and weapons systems are among obvious targets.[6] Cyber attacks against these and other sectors could be conducted with different degrees of intensity, ramping up to the point where they would cripple the country and, potentially, block a coherent national response.[7] The aftermath of the terrorist attacks of September 11, 2001, saw just such blockage, even if not permanent, when the information infrastructure had not been hit.

The national security community has recognized the danger. It has designated cyber as a new domain of warfighting, but other Executive departments and agencies with lead responsibility have failed adequately to keep pace with the cyber threat. While Russia, Iran, and North Korea, among others, pose substantial cyber threats, China stands out because of the extent of its investment and innovations in information technologies.[8] Beijing, not only has undertaken substantial investment in these capabilities, but also it has implemented organizational changes that integrate educational institutions and commercial enterprises and the military and intelligence services in developing and using these capabilities.[9]

Even the best defensive cyber systems in place today only can provide resilience against technologically crude threats; they are not designed to protect the broad attack surface against technologically sophisticated threats to operating systems and related software of the type China has prepared itself to conduct. Such threats are becoming increasingly numerous. Artificial intelligence (AI) and false-flag operations greatly increase the risks and continue to develop at a rapid pace. As a result, the United States truly is vulnerable to a digital Pearl Harbor.

Use of Cyber vs. Kinetic Weapons

For an attacker, cyber weapons and tools present an attractive option to kinetic weapons. For one thing, they are much less expensive and have a far shorter development and production cycle. Equally important, cyber can "scale" from covert operations or espionage where there is plausible deniability at the outset to larger scale operations. This ability to ramp or dial up or down attacks depending on goals and adversary responses increases cyber's appeal as a weapon. Government and industry recognize the possibility of such intensely destructive cyber-attack and information warfare that would dwarf the most skilled past uses of propaganda and active measures.[10]

Attacks against the cyber infrastructure can bring a society to a halt.[11] It is essential, therefore, that the United States urgently deploys the necessary organization, infrastructure, and tools to detect and meet the threat before it becomes a reality – Pearl Harbor again. Both government and industry acknowledge the possibility of such intensely destructive cyber-attack and information warfare that would dwarf the most skilled past uses of propaganda and active measures.[12] It is entirely possible, and some would say likely, that a future conflict would be "hybrid warfare" – a kinetic campaign accompanied by information and cyber operations.[13]

The Growing Cyber Threat from China

The most serious hostile actors such as China have invested heavily over a period of years to develop these capabilities. China's Military-Civil Fusion (MCF) program integrates educational institutions. h military and intelligence services, and the commercial sector. The goal is further development of cyber capabilities, sectors, and workforces.[14] Here the Chinese are also employing advanced AI technologies to achieve powerful new attack capabilities.

Intelligence to Meet the Cyber Threat

As in the case of Pearl Harbor, a major concern needs to be whether the nation is providing the focus and the resources to monitor the threat.[15] In the current cyber context, the United States needs to focus on the development of hostile cyber capabilities and new forms of cyber attack. Existing law, chiefly Titles 10 and 50 of the U.S. Code, and Executive orders impose responsibility for data collection and, threat assessment on the Intelligence Community, specifically, NSA and CIA. Law and regulation, moreover, grant authorities to act to these and other government agencies.[16]

To strengthen their ability to discharge its collection and assessment responsibilities, the Intelligence Community should exploit the types of threat which these agencies have dealt with in the past. Organization, staffing and support need adjustment to provide effective threat detection and analysis. Preliminary research already conducted under DARPA sponsorship that has demonstrated how to collect and exploit data from China and elsewhere. Those engaged in this research have developed special AI tools that make analysis and exploitation possible.

Other departments and agencies presently charged with cybersecurity in the broadest sense, reaching across social and economic sectors, seemingly lack the legal tools necessary to prepare against digital attack and to repair cyber vulnerabilities. Even the Intelligence Community, which has the necessary legal authority, needs to undertake significant changes in its

approach and devote additional resources to the problem. The United States can easily afford the cost.[17]

Reducing Vulnerability and Increasing Resilience to Cyber Attack

It is essential to anticipate the possibility of a multi-faceted, Internet-, and computer-based attack. Adverse states now employ advanced AI technologies to provide powerful attack capabilities, adding, exponentially, to the danger. For an attacker, the use of cyber weapons and tools presents an attractive alternative to a kinetic attack. Unlike a kinetic attack, cyber permits scaling of deniable covert operations or espionage to large scale operations.

The cost of the development and deployment of relevant technologies, moreover, is exceedingly low compared to sophisticated kinetic weapons.[18] Government and industry acknowledge the possibility of intensely destructive cyber-attack and information warfare that would dwarf the most skilled past uses of propaganda and active measures.

To meet the challenge of a potentially devasting cyber attack he nation needs to take effective action to make the attack surface itself less vulnerable before being hit. The Internet itself needs to be hardened. The Internet continues to operate on protocols that are decades old and, despite updates such as Ipv4 and Ipv6, still highly vulnerable to attack. No common, safe standards for Internet security exist. Institutions to create and enforce such new standards do not yet exist. The same can be said for code development where needed standards have yet to be developed or enforced.

While the evolution of net-based cryptocurrency has forced some needed modernization, such improvement has yet to apply to the broader attack surface.[19] The nation needs to create and seriously fund institutions focused on code that is resilient. New institutes at academic institutions or expanded efforts at the existing FFRDCs and national laboratories are needed.

2. The Cybersecurity Mission

Cybersecurity as a New National Security Challenge

Meeting the cybersecurity challenge and avoiding a digital Pearl Harbor requires a serious understanding of the actual mission and how it can effectively be assigned to the multiple agencies and offices now involved.[20] This is a relatively new type of national security challenge and a threat environment that has increased exponentially over the last few years.[21]

At a minimum, heightened interdepartmental coordination is needed to address the potential of a major attack using advanced code development and insertion into critical software and hardware systems. The present technological context of extraordinarily rapid change and threat development makes organizational agility imperative.

Effective interagency coordination is essential and should lead to real partnership, especially between the Defense and Intelligence components with Title 10 and Title 50 authorities[22] and the ability to design and execute technical programs to collect, analyze, and respond to hostile code development ***before*** it is used to attack the nation.[23]

Assignment of Cybersecurity Missions and Roles

At present, none of the various agencies that have been given parts of the overall mission has seriously addressed the increasingly sophisticated capabilities that would figure in a major attack on critical U.S. infrastructure. The capabilities include malicious code development. Foreign states are organizing themselves to achieve and use such capabilities and funding this development heavily.

This situation, in part, is the result of the speed with which this threat has evolved and underlies the need for organizational changes within the existing departments, agencies, and services responsible.[24] The Department of Homeland Security, the Department of Defense, the Intelligence Community, and federal law enforcement have different and sometimes competing missions in the cyber area. They need to be harmonized.

At the outset of the Internet era, hacking and malicious activity was largely the domain of bored high school kids and evolved as a criminal enterprise. While cybercrime remains a concern, the threat from foreign powers needs to be viewed in national security terms. The more recent transition to foreign espionage and cyber warfare potential resulted in the multiplicity of agencies involved.[25]

Improvements in efforts at NSA, CIA, and the new Department of Homeland Security (DHS) collection of Internet-based information in the wake of the 9/11 terrorist attacks have not kept pace. Despite the creation within DHS of the Cybersecurity and Infrastructure Security Agency (CISA), there has been a fundamental and ongoing failure effectively to collect and analyze data on the foreign state cyber threat. A key part of this is the lack of software tools and

AI technology needed to detect and counter preparations for devasting cyber attacks before they become reported incidents.[26]

Few cyberspace analysts make recommendations on how to achieve "integrated deterrence" or strategic integration.[27] Coupled with these failures has been a concurrent failure to develop the needed software tools to detect and counter devasting cyber attacks before they become reported incidents.[28]

One recent effort has been the creation of the Office of the National Cyber Director withing the Executive Office of the President to advise the President on matters related to cybersecurity.[29] Established in 2021, this office has an authorized staff of 75, but has no actual programs of its own or any operational authority. Thus far, its only accomplishment has been the production of the 2023 *National Cybersecurity Strategy,* which ignores the prospect of a devastating cyber attack and the various ways it might occur.[30]

Key Missions of the Department of Defense

While the technologies that created the Internet and cyberspace began as DARPA research projects in the 1960s, security was not seen at the time as a major concern.[31] At the time nobody at DARPA – or anyplace else – envisioned the technology revolution that would take place, or the explosive growth that would take place as every governmental, commercial and private sector organization adopted the new technologies while rapidly abandoning all vestiges of the analog world.

Until recently DARPA made limited investments in cybersecurity, and focused on lower level threats seen at the time with no attention given to the possibility that hostile foreign actors would develop cyber espionage or cyber warfare capabilities. The responsible U.S. intelligence agencies paid little to no attention to the fact that an adversary might actually use the Internet, let alone look to attack the evolving U.S. cyber ecosystem. The 1990s were a "lost decade" for serious cybersecurity efforts.[32] Programs that did exist were underfunded, and others that were needed were never created.[33]

Organizationally the Department of Defense has been more responsive in recent years to the emerging cyber threat with an updated policy, as well as the creation of the U.S. Cyber Command (CYBERCOM) and cyber components within each of the military services.[34] At the same time these Defense Department components lack the supporting intelligence infrastructure and technology base to effectively execute this defensive and offensive mission.

While NSA and CYBERCOM could have expanded collection against this evolving threat and developed the AI tools needed to understand and exploit this data, they failed to do so. Available resources have been focused on "incident reporting" – after the fact attacks – and not on either the foreign infrastructure developing hostile malware or malicious code development.[35] Further, giving a cybersecurity mission with the civilian CISA has added a level of bureaucratic confusion that has impeded the ability of the Defense Department and the Intelligence Community to operate effectively in the cyber domain.

Beyond government, U.S. financial institutions, universities, healthcare providers, power companies, just to name the most obvious, have different missions they need to understand and

therefore different vulnerabilities. They also face different kinds of threats. The urgency for mission definition in each sector and research into, and intelligence about, vulnerabilities and threats cannot be overstated.

3. Chinese and Russian Cyber Operations

It is useful to examine Chinese and Russian cyber operations as examples of different, sophisticated approaches to the cyberlandscape that illuminate both the threat and the ability to control information flow in the Internet environment.

Chinese Cyber Operations

For more than a century, Chinese leaders have valued access to technology and information to support their national objectives and military capabilities. The Chinese Communist Party (CCP) has always understood the importance of controlling information to guarantee its domestic position and maximize its ability to manage competition and conflict. Starting in the 1970s, China moved to acquire technologies in order to collect, store, process, and manage information.[36] Today, the success of the country's cyber and communications development is most visible in areas such as 5G (communications) and AI.

The People's Republic of China (PRC) has invested substantial sums in technologies related to surveillance, espionage and cyberwarfare.[37] China's cyber operations reflect major advances made in these areas. China has shaped and reshaped its national cyber ecosystem, which it exploits in new and innovative ways.[38] The mechanism used by the PRC is their integrated Military-Civil Fusion (MCF) program, which has greatly expanded China's cyber capabilities in intelligence, espionage, deception, and cyber warfare.[39]

Personal use of connected devices, such as mobile phones and laptops, and social media and other applications provide the means to use the technology base for information and control. The Chinese government tracks individuals and their behavior. Users are able to access Chinese sites, and versions of U.S. sites, but the government monitors and controls interactions with servers and sites outside China as well.

The technology also has enabled espionage operations on a scale never before imagined. Operations include theft of intellectual property, extraction of personal data, and penetration of strategic systems—activities going well beyond the traditional intelligence mission of stealing secrets for national security purposes. China collects vast amounts of data. It accesses protected networks and commercial enterprises to make China more competitive in world markets.

As part of their long-term competition with the United States, the Chinese government and CCP view collection and hoarding of information as an investment in the future. It is a strategic aim, not merely a near term tactic. In the area of cyberwarfare, Beijing, however, looks at cyberspace in the broader context of information control.

The ultimate objective is, not "control" of cyberspace, but control of information, a vision that dominates China's cyber operations. Chinese military strategists have also begun to discuss the emergence of what they refer to as "intelligentized warfare," which includes the use of information analysis and AI technologies to target an adversary's "cognition."

China's cyber capabilities and operations have increased exponentially to the point where they pose a highly significant national security threat to the United States and all China's perceived adversaries. The size of the attack surface exponentially increases the risk from such cyber operations and capabilities as China continues to invest huge sums in this technology path. It is clear that the threat will continue to become even greater than it is now.

Knowledge of these details of the Chinese cyber strategy and threat need to become a central part of the U.S. national security discourse with respect to cybersecurity. All U.S. institutions need to assess their vulnerabilities and manage their risks in light of these Chinese practices. The same is true with respect to Russian cyber operations.

Russian Cyber Operations

Russian use of information and the Internet has strong historical roots. For more than a century, Russia has used forgeries, disinformation, and falsehood-propagation as an important military and intelligence tool, using "active measures" (*aktivnye meropriyatiya)* as covert and deniable political influence and subversion operations, from corruption and disinformation to assassination and sponsorship of coups.

This history stretches to the time of the Tsars. Throughout the Communist period, Russia used "active measures" including front organizations and spreading false information. In the context of the Internet and advanced information technologies, the Russians emphasize deniability, blur the lines between public diplomacy and propaganda, and use disinformation as a form of political warfare.[40]

Russia views cyber differently than its western counterparts. Russia under Putin is engaged in what it perceives as an ongoing, existential struggle against forces threatening the regime. This perception is increasingly driven by paranoia and conspiratorialism, particularly about "color revolutions" that the Putin regime fears within Russia. The Putin regime also believes in using asymmetric tactics, such as executing assassinations and running disinformation campaigns, to achieve its aims at home and abroad.

Hence, the Russian government sees the Internet and the free flow of information it engenders as both a serious threat and equally serious opportunity. The Russian government, perhaps even more successfully than its Communist predecessor, controls access to information. Reporting on Moscow's ability to control public knowledge of the Ukraine war shows that government can control Internet-based access to information.

Russian military theorists avoid using the terms cyber or cyberwarfare, preferring to see cyber operations in the broader framework of information warfare. This holistic concept includes computer network operations, electronic warfare, psychological operations, and information operations. Consistent with Soviet notions of combating ongoing threats from abroad and within, Russia views the struggle over "information space" as constant and unending.

Offensive cyber operations therefore play a large and increasing role in Russian military operations and strategic deterrence. While the Russian military and intelligence services were slow to embrace cyber operations, the government has made significant investments in the last decade and continues to bolster offensive and defensive cyber capabilities. Russian patriotic

hackers, front groups, and cyber-criminal syndicates, added to military and intelligence capabilities, have become central to Russian offensive cyber operations. They provide easily mobilized, anonymous, and deniable cyber assets and actors.

Perhaps the most infamous Russian information warfare proxy group is the Internet Research Agency (IRA), a troll farm initially based out of St. Petersburg, Russia and funded by the late Yevgeny Prigozhin, oligarch and former head of the private military company Wagner Group. The IRA worked to advance the Kremlin's objectives abroad by, among other things, creating fake news articles and posts and then falsely amplifying them on U.S. social media platforms. It has in the years since opened covert outposts outside of Russia, such as in Mexico and Nigeria, to spread disinformation in the West.

While Russia has used hackers and criminal networks in the past, evidence now suggests that they are being augmented, if not entirely replaced, by FSB (Russian Federal Security Service (successor to the Soviet KGB)), GRU (Russian Military Intelligence Organization), and others including independent hackers and criminals. The Russian model includes elements of the intelligence services and "external" contract activity, principally the IRA.

Other commercial operatives, such as Positive Technologies, and Kaspersky, are known to support government requirements, in some cases provide direct support to Russian government operations in the FSB and GRU and engage in the international sale of commercial security products. For example, Positive Technologies annually hosts the largest hacking conference in Russia, which the Russian security services use as a venue to recruit hackers to work for the Russian intelligence community.

Moscow also views cyber operations as means of disruption for disruption's sake. It can degrade an enemy's military communications, disrupt a foreign company's operations in Russia, and achieve other objectives by means that do not amount to an overt use of military force and still retain the ability claim plausible deniability.

4. Reducing Vulnerability and Increasing Resilience

Life in The Digital World

The rapid transition of most U.S. institutions to the digital, connected world makes the multi-faceted national infrastructure subject to catastrophic attack and failure. While this digital revolution was taking place, the realm of cyber "attack" and threat also evolved from bored students who engaged in hacking to major criminal organizations and hostile foreign intelligence services and militaries.

This change in the nature and level of threat was not appreciated as worldwide use of the cyber ecosystem exploded. In part, this failure of understanding can be attributed to the speed in which this threat evolved, and in part to the relatively glacial pace in which the federal bureaucracy adapts to changing missions and direction of resources to meet such rapidly evolving threats.[41]

Meeting this challenge and enhancing the security of this infrastructure requires changes in the national approach to organization and decision-making, improved threat detection and analysis, enhanced resilience, hardening of the cyber infrastructure, and preparation for future cyber disasters.

Well into the first decade of the Internet the sophisticated view was that financial services institutions and other businesses would solve the technical security problems in their self-interest. Insurance companies would enforce adoption of best practices on commercial actors and so heavy-handed government action was not necessary. Other sectors and the government itself would take a free ride on the security innovations and investments driven by commerce.[42] This assumption turned out not to be true for a variety of reasons.

Rethinking the National Approach to Cybersecurity

After World War II, the United States changed its approach to national security, responding to major changes in the threat environment and the technologies involved as well as to the disappearance of alternative great powers that could maintain the peace. The 1947 National Security Act created the Department of Defense and the Air Force, as well as the Central Intelligence Agency to meet an emerging Soviet threat and the potential use of nuclear weapons by the Soviet Union.[43] Despite the fact that cyber threats merit similarly serious institutional responses, the United States has yet to take analogous action.

The technological "surprise" of the Soviet space and missile program of the 1950s led the President to direct a major review of all U.S. agencies and programs and how the nation would respond to this major change in the threat.[44] As a result. major changes were made in the military services while the Intelligence Community created the National Reconnaissance Office (NRO) as one means to collect much-needed data. CIA created new offices and centers responsive to the

emerging threat, supported by a robust external infrastructure. CIA also undertook substantial organizational and staffing changes to deal with the evolving Soviet threat and produce timely, accurate assessments.[45] The National Security Agency (NSA), newly created within the Department of Defense by Presidential Order in 1952, undertook other needed efforts in the SIGINT area.[46]

In addition, Congress authorized major investments in a supporting analytical infrastructure to assist the Defense Department and the Intelligence Community. It included the national laboratories, federally funded research and development centers (FFRDCs), a substantial number of private-sector contractors, and university centers. Further supporting the research and development needed were the creation of ARPA, NSF and funding of university research under the National Defense Education Act.[47]

Following the end of the Cold War and demise of the Soviet Union, the national security community failed to take similar steps to respond to radical changes in the threat, as the 9/11 attacks and subsequent analysis revealed.[48] Adding a new federal department (DHS) was one part of the response, as were changes in federal, state and local law enforcement. None of these dealt seriously with the evolving cyber threat. The result remains a collage of federal departments, agencies, and military services attempting to deal with parts of the cyber threat – some of the efforts overlap, and others are simply nonresponsive to the actual threat.

In light of the magnitude of the threat, it would be useful to have both the Executive and Congress undertake an assessment of the overall organizational structure for dealing with the threat and the technologies needed to detect attacks before they happen and respond accordingly. At a minimum, a serious bi-partisan commission with a short timeline to do research and report to the President and Congress would be a useful step. The current mantras of incident reporting and public-private partnerships do little in fact to deal with the risk of a digital Pearl Harbor. The United States would do well to adapt some of the ways it responded to the Cold War—national laboratories, FFRDCs, and the like—to address cyber rather than reinvent the wheel.

One positive development has been a growing community of national security experts looking at the role of deterrence related to cyber warfare. Experts in and outside government have studied the prior experience of the nation in dealing with the Cold War and how these concepts can be translated into dealing with the new challenge of deterring cyber attack.[49]

Improved Threat Detection and Analysis

The DARPA SocialCyber, HARDEN and HAMILTON programs, among others, have demonstrated the possibility of reducing vulnerability to major cyber attack through early detection and analysis of hostile code development. This research has integrated extensive collection of code artifacts, patches and other postings along with the development of a set of AI tools that enable identification of malicious code from a large body of data.

Along with the data collection and AI tool development has been an integrated analysis of the organization, institutions and individuals involved in malicious code development utilizing original source materials and graph databases. It is essential that this strategy and tool set be transitioned to the responsible Intelligence Community elements for use on an ongoing basis.

DARPA was the initial home of the Internet and for decades has engaged in research on related network and software technology. It has long supported Intelligence Community partners at NSA and CIA. Current DARPA programs, including those noted above, have taken an approach that is not currently being applied to the problem by the appropriate executive branch organizations. This integrated approach has several key elements:

- Ongoing collection of open source data such as public email, code artifacts, communications, and postings from hostile nations (such as China and Russia) that may be malicious code to be used in activities such as espionage and cyber warfare.
- Use of AI tools applied to the database to identify both malicious code as well as specific individuals who are "contributors" of potentially malicious code.
- Application of graph database tools to demonstrate links between malicious code and code contributors.
- Integrated use of technical experts who are also involved in the development of offensive cyber tools for the U.S. that understand this software.
- Use of regional experts with native fluency in Chinese and Russian as well as expertise in cyber operations, to examine the supporting infrastructure in hostile nations as well as specific messages in the database.

The United States currently lacks such an integrated approach. It also lacks an alternative approach to detect and counter hostile code development. While the responsible agencies may collect some similar data, they still lack the associated AI tools to evaluate the data on an ongoing basis and do not have programs in place to develop them. This means the United State lacks an effective means to prevent or mitigate a digital Pearl Harbor.

Enhancing Resilience and Hardening of the Cyber Infrastructure

For several decades computer scientists associated with DARPA and elsewhere have looked at issues related to modernizing the Internet and enhancing the resilience of the existing infrastructure. Even though the Internet has gone through a period of explosive growth worldwide that was unimagined at the outset it continues to operate with many of the technologies and protocols developed in the 1960s. Even the current IPv4 Internet protocol is a product of the 1980s.[50] Its successor, IPv6, is still being deployed and lacks the type of resilience that most experts believe is essential.

Resolving this aspect of the problem lies in the hands of several worldwide bodies and outside the control of any U.S agency or intelligence service. Whether the worldwide infrastructure will continue with periodic upgrades such as IPv6 which leave many vulnerabilities unresolved, or whether a new and possibly parallel Internet 2.0 will come into being remains an open question.[51] At the same time, the U.S. government could take steps to build, adopt, and mandate for Americans an Internet 2.0. Given U.S. international influence, such a step should not be ruled out, although it currently lacks broad international support.

Apart from the backbone Internet infrastructure itself, software ranging from operating systems to a myriad of applications remain vulnerable to hostile cyber attack. Important findings

from the DARPA SocialCyber analysis as well as other recent research has been that popular operating systems, such as Linux, are vulnerable to "contributors" submitting patches and other changes that may in fact introduce malware into the system. An essential part of the intelligence mission here is to monitor these contributions and their contributors with specialized AI tools developed for this task.[52]

Most operating systems and applications are vulnerable. They therefore should be reviewed for specific vulnerabilities, and there need to be plans made for the event they are attacked. The spate of ransomware attacks in recent years at least provides some insight into how failure at some level might impede organizations' operations, such as that of pipeline companies or hospitals, and suggests what can be done to improve resilience here. Mitigation might take the form of separate servers and software or movement to a more protected cloud environment.[53]

Development of Resilient Computer Code

To support the development of a more resilient cyber infrastructure one useful concept would be to provide far greater resources for software engineering institutes and similar institutions within the U.S. that would further develop much needed standards and data formats for documents and other digital media.[54] At present, there are virtually no common or accepted standards for either data formats or code development. The lack of standards renders the U.S. cyber ecosystem more vulnerable to hostile attack than otherwise would be the case.

Exactly how this critical task can be accomplished should be a matter of major concern for both the Executive branch and Congress. Just as the nation responded to the Soviet threat and new technologies during the Cold War, the United States needs to create a broader scientific and technical infrastructure that is able to produce computer code that is far more resilient in the evolving threat environment.

There are multiple approaches to meeting this challenge. As in the past, the United States may be best served by using several simultaneously. Certainly, new institutes at academic institutions can play an important role.[55] Another element might be to expand efforts at the existing FFRDCs and national laboratories.[56] At the same time, the supporting commercial contractor base as well as major firms such as Microsoft, Google, and Oracle, just to name a few, need to become an essential part of the process. Responsible government agencies need to be continuously involved, not only as sponsors, but also as overseers to ensure that the process of code development meets the requirements of the evolving threat.

Meeting this challenge needs to remain a core mission for agencies like DARPA and the research components of the Defense Department, the military services, and the Intelligence Community. Such agencies and offices have the internal structure and program management capability to execute this technical mission and need adequate resources to do so. Successful initiatives need to move to places where they can become operational on a sufficiently large scale to benefit the entire cybersecurity effort.

Longer-Term Measures to Prepare for a Cyber Disaster

Although no major or devastating cyber attack has taken place, the threat remains and will continue to grow. Over the longer-term measures need to be taken in order to prepare the country

for the growing possibility of a digital Pearl Harbor and respond effectively in the event it happens. Some of the most important measures include:

- Organizational changes which assign the lead to a department, agency and offices having the legal, technical, and management capability to execute an effective cybersecurity program.
- Development of a supporting infrastructure within the government, as well as an adequately funded external base of national laboratories, FFRDCs, contractors, universities, and commercial infrastructure.
- Explore what AI technologies can do to meet emerging threats to critical sectors to ensure that the U.S. maintains an advantage and the ability to provide the needed resilience.
- Engage in realistic "stress testing" and "war gaming" of potential high-end cyber attacks.
- Provide for the development of resilient data formats and standards for code development through new and adequately funded software engineering institutes and others.
- Work with Congress to ensure that both funding and oversight of essential activities are supported.

Winston Churchill's admonition, "action this day," must be the watchword.

Notes

[1] See Emily O. Goldman and Michael Warner, "Why a Digital Pearl Harbor Makes Sense . . . and is Possible," in George Perkovich an Ariel E. Levite, (ed.), *Understanding Cyber Conflict: Fourteen Analogies* (Washington: Georgetown University Press, 2018). The most extensive historical discussion of the 1941 Pearl Harbor attack is Gordon W. Prange with Donald M. Goldstein and Katherine V. Dillon, *Dawn We Slept: The Untold Story of Pearl Harbor*, (Revised Edition), (New York: Penguin, 1991). See also, US Congress, Joint Committee on the Investigation of the Pearl Harbor Attack, "Investigation of the Pearl Harbor Attack," 79th Congress, 2d Session, 1946, and Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962). Much of the discussion about the Pearl Harbor attack relates to intelligence warning and how it was handled at the time.

[2] Every aspect of modern life depends on the Internet. If the system were not global, if huge institutions did not depend on what presently exists, it would be a relatively easy matter to replace the existing Internet with protocols that were created with security in mind. That would be desirable but difficult to accomplish. Rebuilding systems would be a helpful step in managing risk. Some years ago, for example, one of the Defense Department educational institutions confronted the problem of a substantial number of hacking efforts targeting its old, jury-rigged information technology systems and networks. But the institution lacked the operating funds to replace and rebuild the systems. Those in charge would not treat replacement and rebuilding as a necessary capital expense as important as replacing a leaky roof. The result was more inadequate patchwork. Until the United States recognizes the need for that kind of capital investment and the U.S. government builds, uses, and mandates Internet 2.0, the nation needs the fact that it remains vulnerable to potentially devastating cyber attack.

[3] It is possible to these existing or potential flashpoints the threat posed by North Korea and the risk of a Chinese attack on Taiwan.

[4] See Grange, *op. cit*. and Wohlstetter, *op. cit*.

[5] See Michael W. Kanzelberger, *American Nuclear Strategy: A Selective Analytic Survey of Threat Concepts for Deterrence and Compellence*. (RAND N-1238-AF, September 1979), Joseph A. Cernik, "The Current United States Targeting Doctrine of Nuclear Weapons: An Explanation and Analysis," *Presidential Studies Quarterly*, (Winter - Spring, 1976), and Milton Leitenberg, "Presidential Directive (P. D.) 59: United States Nuclear Weapon Targeting Policy," *Journal of Peace Research*, (1981).

[6] For example DARPA, working in cooperation with the Treasury Department, has recently launched Project HAMILTON looking at the vulnerability of the nation's financial sector to a major cyber attack.

[7] NSA's Director publicly recognized the problem a decade ago. See Keith B, Alexander, Emily Goldman, and Michael Warner, "Defending America in Cyberspace," *The National Interest* (November/December 2013). More recently see, John Ratcliffe and Abraham Wagner, "U.S. Needs New 'Manhattan Project' to Avoid Cyber Catastrophe," *Newsweek* (May 18, 2022) and Tom O'Conner, Naveed Jamali and Fred Guterl, "Will Putin's Hackers Launch a Cyber Pearl Harbor—and a Shooting War? *Newsweek* (June 18, 2021).

[8] Most analysts agree that the four key hostile states are China, Russia, Iran and North Korea. While the present analysis gives examples from the first two, this is not to say that the threat posed by the others can be ignored.

[9] See *China's Cyber Power and Military-Civil Fusion* (New York: Margin Research, February 2023).

[10] Apart from a skilled workforce, the only hardware required are computers and bandwidth. Compared to kinetic warfare's guns, bombs, tanks, aircraft, missiles, ships, and other costly equipment, the cost differential is less than trivial.

[11] See Abraham Wagner, Thomas Garwin, Nicholas Rostow, Sophia d'Antoine and David Aitel, *DARPA Cybersecurity Planning, Technologies for Keeping the Nation Safe* (Los Angeles: Center for Advanced Studies on Terrorism, 2018). Note one recent example The hacking operation, a Chinese operation code-named "Volt Typhoon," has been active since mid-2021 and "could disrupt critical communications infrastructure between the United States and Asia region during future crises." See also, "Chinese malware targeting critical infrastructure, Microsoft and U.S. government warn," *CBS News* (May 23, 2023).

[12] Apart from a skilled workforce, the only hardware required are computers and bandwidth. Compared to kinetic warfare where guns, bombs, tanks, aircraft, missiles, ships and other costly equipment is required the cost differential is less than trivial.

[13] Going back to World War II and before this was already true, importantly minus the Internet. This has been a major part of Soviet strategy for many decades and is evident now in Russian operations in the Ukraine. Clearly most hostile powers have plans that include cyber operations as part of an overall strategy.

[14] See *China's Cyber Power and Military-Civil Fusion* (New York: Margin Research, February 2023).

[15] Extensive analyses of the intelligence and warning related to the 1941 Pearl Harbor attack were undertaken. See Prange, *op cit*., and Wohlstetter, *op. cit,* At the time critical intelligence was obtained from the highly classified decrypted MAGIC intercepts of Japanese communications. For technical reasons, the data about the impending Japanese attack did not get to Hawaii in time. It is worth noting that this important intelligence work by William Friedman and his team at the U.S. Army Signal Intelligence Service (SIS) was not a major, well-funded activity. Friedman's entire team consisted of seven employees, and an annual budget that never exceeded $17,400.

[16] See Abraham Wagner and Nicholas Rostow, *Cybersecurity and Cyberlaw* (Durham: Carolina Academic Press, 2020).

[17] In the United States, which now spends in excess of $85 billion annually on its intelligence services, it is difficult to see that so little is being done effectively to address this threat despite some specific cases to the contrary. See, for example, Ellen Nakashima, "Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election," *The Washington Post* (October 9, 2020).

[18] See fn. 10 above.

[19] See "What is the Difference Between DeFi and Web3?," *Cryptopedia* (March 10, 2023).

[20] An effort to analyze the roles and missions of various agencies and offices was begun in 2018 at the NSC with a view toward an Executive Order that would be an analog to E.O. 12333 which set out the roles and missions for the Intelligence Community.

[21] It is possible to draw an historic comparison to the development of the atomic bomb, where U.S. intelligence saw the bomb program in Nazi Germany and at the President's direction initiated the MANHATTAN project to develop a nuclear weapon before any hostile nation had produced or used one. See Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1986). Similarly, it is also possible to draw a comparison to the nation's response to the Soviet Union's development of nuclear weapons and delivery systems, including long-range bombers and missiles. This response took

place over several decades and included millions in intelligence systems to monitor the threat and many more millions in defense spending to counter the threat.

[22] Title 10 of the United States Code outlines the role of the U.S. armed forces and provides the legal basis for the roles, missions and organization of each of the military services as well as the United States Department of Defense. Title 50 of the United States Code provides a comprehensive program for the security of the nation and sets out integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security including the Department of Defense, the three military services, and the intelligence agencies.

[23] The set of technologies that created the Internet and related communications began with research projects at what was then the Advanced Research Projects Agency (ARPA) beginning in the 1960s. At the time nobody at ARPA—or anyplace else—envisioned the technology revolution that would soon take place, With the transition from the experimental ARPAnet to the Internet after 1990 the explosive growth was unimaginable, as every governmental, commercial and private sector adopted the new technologies while rapidly abandoning all vestiges of the analog world.

[24] It is worth noting that while the basic structure for national security was set forth in the 1947 National Security Act, issues of roles and missions within the Intelligence Community remained for decades and were "sorted out" in Executive Order 12333 signed in December 1981 by President Ronald Reagan.

[25] See Wagner and Rostow, *Cybersecurity and Cyberlaw, op. cit.*

[26] Too much of the current U.S. cybersecurity strategy has focused on "incident reporting" – i.e. documenting attacks after they happen rather than preventing them. See The White House, *National Cybersecurity Strategy* (March 2023).

[27] See, for example, Joseph L. Billingsley (ed.), *Integrated Deterrence and Cyberspace* (Washington: National Defense University Press, May 2023).

[28] A developmental data base (OVERWATCH), currently holding some 200GB of foreign data, largely from China, has been created under the DARPA SocialCyber program and utilized for AI tool development and analysis, resulting in the REAGENT AI tool set. The CISA Vulnerability Directorate appears to be largely unaware of this data and the AI tools developed to understand and exploit to defend against attacks.

[29] The position of National Cyber Director was established under the 2021 National Defense Authorization Act on the recommendation of the Cyberspace Solarium Commission, a congressionally authorized panel convened in 2019. Located within the Executive Office of the President it is charged with "programs and policies intended to improve the cybersecurity posture of the United States, ... diplomatic and other efforts to develop norms and international consensus around responsible state behavior in cyberspace" and other matters related to cybersecurity." See David Sanger, "Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul," *The New York Times* (March 11, 2020).

[30] The White House, National Cybersecurity Strategy (March 2023).

[31] At the time the agency's name was ARPA (without the Defense). See also, Sharon Weinberger, *The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency That Changed the World* (New York: Random House, 2017), and Annie Jacobsen, *The Pentagon's Brain: An Uncensored History of DARPA, America's Top Secret Military Research Agency,* (New York: Hachette, 2015).

[32] An effort undertaken by the Director of Central Intelligence (DCI) in the mid-1990s to examine the *Global Information Infrastructure (GII)* was abruptly terminated, for no good reason whatsoever.

[33] Even at DARPA early efforts to support Defense Department and Intelligence Community elements in the area of Internet exploitation were flatly turned down. Following the 9/11 attacks, Secretary of

Defense Donald Rumsfeld personally had to change this policy. A programmatic history of these efforts has yet to be written.

[34] *Department of Defense Strategy for Operating in Cyberspace* (July 2011). See also *Department of Defense Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (November 2011). Most recently CYBECOM has begun to examine its next-generation weapons platform.

[35] Note that what was accomplished as a research effort under the DARPA SocialCyber program could and should have been done by DoD and the Intelligence Community but was not. This involved not only computer scientists, but social scientists and graduate students with cyber skills as well as native fluency in Chinese and Russian. See Dave Aitel, et al, *China's Cyber Operations: The Rising Threat to American Security* (New York: Margin Research, August 2022), and *China's Cyber Laws and Regulations* (New York: Margin Research, February 2023).

[36] See Aitel, *op. cit.,* and *China's Cyber Laws and Regulations, op. cit*.

[37] NSA's Cybersecurity Director Rob Joyce has recently been quoted as saying that "The PRC's goal is developing capabilities to disrupt critical infrastructure in the event of future conflict" in Sydney J. Freedberg, Jr., "Chinese 'Volt Typhoon' hack underlines shifting Beijing's Targets, *Breaking Defense* (June 7, 2023). See also, *China's Cyber Power and Military-Civil Fusion* (New York: Margin Research, February 2023). See also, Dean Cheng, *Cyber Dragon: Inside China's Information and Warfare Operations* (Santa Barbara: Praeger, 2017), Michael Pillsbury, *The Hundred Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt & Co., 2015), Nick Beecroft, *The West Should Not Be Complacent About China's Cyber Capabilities* (Washington: Carnegie Endowment for International Peace, July 6, 2021), Gordon G. Chang, *The Great U.S.-China Tech War* (New York: Encounter Books, 2020) and Anthony H. Cordesman, *China: The Civil-Military Challenge,* (Washington: Center for Strategic and International Studies, January 4, 2022). See Lyu Jinghua, *What Are China's Cyber Capabilities and Intentions?* (Washington: Carnegie Endowment for International Peace, April 1, 2019) and China State Council, *New Generation Artificial Intelligence Development Plan* (Beijing, July 2017). See also Katharin Tai and Yuan Yi Zhu, "A historical explanation of Chinese cybersovereignty," *International Relations of the Asia-Pacific* (2022) and Nicholas Lyall, "China's Cyber Militias," *The Diplomat* (March 1, 2018).

[38] See *China's Cyber Power and Military-Civil Fusion* (New York: Margin Research, February 2023).

[39] *Ibid.*

[40] See Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner, *Russia's Cyber Operations: A Threat to American National Security* (New York: Margin Research, 2023).

[41] If, for example, if one were to look back at the overall national intelligence budget (NFIB) in the early 1990s it would be possible to conclude that no subject of either intelligence or law enforcement interest would ever use a cell phone or the Internet. Offices and programs to meet these evolving challenges were largely nonexistent. A serious history of this programmatic evolution has yet to be written and would likely run into classification problems if ever done.

[42] These include the different situations of different sectors, the capacity of businesses to absorb losses as a cost of doing business, the possibility of zero-day exploits, the prevalence of social engineering attacks, and other factors. The nation now knows better.

[43] Pub.L. 80-253, 61 Stat. 495, enacted July 26, 1947. The 1947 Act created the Central Intelligence Group (CIG) to replace the Wartime OSS intelligence service which was eliminated by President Turman's Executive Order in 1946. The 1948 Central Intelligence Act changed the name to the Central

Intelligence Agency. See Charles A, Stevenson, "The Story Behind the National Security Act of 1947" *Military Review* (May-June 2008).

[44] See George B. Kistiakowsky, *A Scientist at the White House* (Cambridge: Harvard University Press, 1976).

[45] Changes within the CIA include the Office of Strategic Research (OSR) created in 1967 as well as the Strategic Evaluation Center (SEC) which proved highly successful over the years. See Robert D. Vickers, Jr., "CIA's Office of Strategic Research: A brief History," *Studies in Intelligence* (March 2018), and Central Intelligence Agency, *National Foreign Assessment Center: Organizational Structure and Functions,* (NFAC Plans and Programs Staff, December 1977, Declassified 2002). Organizational efforts within CIA to deal with cybersecurity and related issues provided far less successful. A history of these efforts, offices and programs remains to be written.

[46] See Thomas L. Burns, *The Origins of the National Security Agency* (United States Cryptologic History, National Security Agency, 1990) (Declassified 2007). In 1959 Congress enacted the National Security Agency Act which provides a separate legislative basis for NSA's activities.

[47] See fn. 29 above.

[48] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (September 2004). Adding a new federal department (DHS) was an effort to deal with the evolving terrorist threat and solve some of the problems identified by the 9/11 Commission in the area of domestic intelligence. Unlike most other nations, the U.S. has no domestic intelligence service (similar to Great Britain's MI-5) and the 1947 National Security Act expressly prohibits one. Efforts following 9/11 to resolve the domestic intelligence issue were not successful. Neither DHS nor the FBI were granted such authority by statute.

[49] See Billingsley, *op. cit.* The authors of the essays in this volume as well as those cited in the footnotes are a good example of the emerging community of experts working on this area.

[50] Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and is still one of the core protocols of the Internet. IPv4 was first deployed for production in 1982 and on the ARPAnet in January 1983 and is still used to route most Internet traffic today, even with the ongoing deployment of Internet Protocol version 6 (IPv6) its successor.

[51] An additional question not often discussed is the physical vulnerability of the infrastructure. The operation of the Internet backbone in the U.S. depends on several core routers that are located in unguarded commercial buildings whose locations are well-known. An adversary could easily destroy some or all of these.

[52] See, for example, Ralph Ramsauer, et. al., "The Sound of Silence: Mining Security Vulnerabilities from Secret Integration Channels in Open-Source Projects," *ACM Proceedings* (November 2020).

[53] See Lily Ablon, et al., *Going Dark: Implications of an Encrypted World* (Los Angeles: Center for Advanced Studies on Terrorism, 2017) and *Cloud Encryption, Privacy and National Security: Legal and Political Context* (New York: Margin Research: January 2023).

[54] One effort in this direction has been the DARPA Safe Documents (SafeDocs) to develop novel and verified programming methodologies for electronic data formats. This will help protect against input attacks trying to prevent the flow of untrusted data to vulnerable software; and testing software with randomized inputs to find and patch flaws triggered by maliciously created inputs.

[55] One excellent example is Carnegie-Mellon University's Software Engineering Institute (SEI), which has supported DARPA and others in the computer security area for decades.

[56] Over the past several years there has been discussion about starting yet another FFRDC to deal with the cybersecurity problem, which has faced considerable resistance within the Congress and elsewhere,

probably for good reason. Some additional tasking and funding to RAND, IDA, CNA, MITRE and others would serve the same purpose at a lower cost.