Meeting the Intelligence Technology Challenge: Getting Out From Behind the Power Curve

Abraham Wagner

Introduction

There is little doubt that the prospect of hostile cyber attacks and cyberwarfare has become a major national security challenge. They are a major feature of the current technological context facing the Intelligence Community and Defense Department that have largely failed to respond effectively to this evolving threat.[1] The very real prospect of a "Digital Pearl Harbor" continues to loom while the responsible Intelligence Community agencies are not collecting, monitoring or analyzing the data effectively. Further, they have not worked with their colleagues in the Defense Department to build adequate defenses or the ability to deter such a hostile attack or to respond effectively to one.[2]

Existing offices and centers are buried under a host of classified special access programs originally designed to protect important "sources and methods" but also serve to obscure the fact that in this critical area the Emperor has no clothes. It is not for lack of resources. Within the $90 billion or so the United States spends annually on intelligence programs there is certainly more than enough to support the needed programs.

Dealing with the cyber threat does not require multi-billion dollar satellites or any similar major investment. It does need serious management attention at the most senior levels and real action to deal with decades of complacency and neglect. The nation cannot rely on out-of-date programs and technologies to meet the evolving threat, or that simply do not exist.[3]

The cyber ecosystem and technologies that shape and drive it are not static. This fact requires the kind of programmatic agility for which governments historically have not been suited except in wartime or in peacetime on an almost wartime footing. Today, everything connected to information technologies that makes a modern society function is at risk: financial services, utilities, energy, distribution mechanisms, healthcare, and weapons systems. This reality creates an enormous and highly vulnerable attack surface. To meet today's and tomorrow's cyber

---

[1] See Nicholas Rostow and Abraham Wagner, *Digital Pearl Harbor: Responses to the Growing Threat* (Margin Research, 2023): John Ratcliffe and Abraham Wagner, "U.S. Needs New 'Manhattan Project' to Avoid Cyber Catastrophe," *Newsweek* (May 18, 2022); Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs* (January/February 2022); and Paul Rosenzweig, "Volt Typhoon and the Disruption of the U.S. Cyber Strategy," *Lawfare* (March 5, 2024).

[2] See, for example, Thomas Garwin, Nicholas Rostow and Abraham Wagner, *Cyber Threats to the Financial Sector: Understanding the Attack Surface* (New York: Margin Research, January 2024).

[3] The decision to assign much of the responsibility in this area to the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security was a major error, CISA lacks not only the authorizing statutes for the mission but also the ability to execute a serious technical program. It therefore is ill-equipped to meet the challenge posed by advanced technological threats, including new AI-enhanced cyber threats.

technology challenge to this set of targets requires the sensible dedication of resources and intellectual effort.

It is useful to consider where the nation is now and how it got into this situation, . At a minimum, programs and technologies are needed to deal with the challenges of today, and a focus also needs to be made on how the cyber ecosystem is evolving and what will be needed to deal with the challenges of the future. To accomplish this it is important to focus on:

- What was done or not done in the past is essential to understanding the evolving cyber threat.
- What is being done now by the responsible agencies to collect against, analyze, and respond to hostile cyber threats, and
- How the cyber threat ecosystem is evolving and what the future threat environment will be five, ten, or 20 years from now.

The Intelligence Community's Sordid History of Dealing with Technology

For several decades, the Intelligence Community has had a poor record of dealing with new technologies. If one looks back at the national intelligence budget in the mid-1990s, for example, it would be possible to conclude that no subject of intelligence, or law enforcement interest for that matter, would ever use either a cell telephone or the Internet.[4] While this sounds preposterous, actual Intelligence Community programs for collection against these two new technologies were either trivial or largely non-existent.[5]

In key technology areas the Intelligence Community was seriously behind the power curve and not supporting essential work in these rapidly evolving new technologies. At a time when the nation, and indeed the world, was being wired with fiber optic cables and cell sites/towers were springing up everywhere the IC continued to focus on copper cable; microwave towers and other communication and information technologies dating back to the 1930s and before.

While NSA was late to the game in dealing with cellular telephone, they ultimately came to grips with this evolving communications technology, putting in place programs to collect and analyze this information.[6] Large-scale collection of Internet traffic, however, does not support the

---

[4] DARPA undertook the transition from the experimental ARPAnet to the public Internet in FY-1990 and as has been well-reported, grew to become a worldwide communication medium at lightning speed. See, for example, Stephen Segeller, *Nerds 2.0.1: A Brief History of the Internet* (New York: TV Books, 1998) for one of the better books on this subject.

[5] The budget for the FBI and other federal law enforcement are not included in the overall national intelligence budget (NFIB), but there were essentially no funds for such programs there either.

[6] Looking at ancient history, in the early 1900s NSA's predecessor initiated a partnership with AT&T for a classified or "black" program to collect against international telecommunications. At a minimum it provided an understanding for the need to collect against phone communications. For some of this history see Thomas L. Burns, *The Origins of the National Security Agency* (United States Cryptologic History, National Security Agency, 1990) (Declassified 2007). CIA's Office of SIGINT Operations (OSO) which also dealt with these technologies at the time is not covered here.

collection specific malicious code artifacts and malware that in many case are not contained in email or postings. Also missing was AI tools to identify malicious code and cyber weapons from a massive amount of extant data.

Programs to deal with the "new" Internet were limited to a handful of people, with virtually no resources, operating within highly restricted security compartments. 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. For its part DARPA, the original home of the Internet, refused to assist the Intelligence Community in addressing the fact that Internet resources could be used by intelligence targets, or even required fundamental security protection for a rapidly expanding universe of net users.[7]

An effort undertaken by the Director of Central Intelligence (DCI) in the mid-1990s to examine the evolution of the cyber ecosystem and what the IC could do to address the problem in the *Global Information Infrastructure (GII)* was abruptly terminated – for no good reason whatsoever. A set of recommendations as to how organizational changes and programs to meet the evolving challenge of the Internet and social media could be met were largely ignored.

The Current Challenge: Dealing with the Digital World

First, it is essential to recognize that the cyber ecosystem enables cheap but devastating hostile cyber actions against society's vulnerable attack surface. While cybersecurity has been a concern for years, rapid operating system advances, for example, quickly render dangerously vulnerable older systems such as those used in ATM machines worldwide. While this problem demands attention from those who oversee and run banks, Government can take steps now that would at least mitigate some of the threats.

It is entirely possible, and some might say likely, that a future conflict would be "hybrid warfare" – a kinetic campaign accompanied by information and cyber operations.[8] Given the worsened geopolitical situation, a cyber attack in service of an actual or impending war, and information operations favorably to alter the geopolitical terrain in advance of kinetic operations should be foreseeable and a matter of concern.

Such measures include the employment of technologies to detect and analyze malicious computer code before an attack. It is possible now also to track those that are developing malicious

[7] 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 and private sector user adopted the new technologies while rapidly abandoning all vestiges of the analog world. Exactly why successive DARPA managers resisted helping their DoD and Intelligence Community partners in dealing with Internet collection to support national security missions is a long story best left for another day.

[8] Going back to World War II and before this was already true, less 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 military strategy. Indeed, both China and Russia make no secret of this.

code. Second, it is crucially important to do much more than we are doing to enhance cyber ecosystem resilience. Resilience by itself decreases vulnerability to attack and increases effective national cyber risk management. The nation cannot afford to wait for a Digital Pearl Harbor or a 9/11 type of attack to improve its cybersecurity posture.

The present cyber context requires enhanced Intelligence Community exploitation of nascent, promising efforts to monitor the development of hostile cyber warfare capabilities, creation of malicious code, and the institutions and individuals involved. Such efforts include new approaches to the misuse of social media and the increase in high technology disinformation and misleading public diplomacy. 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.

Unfortunately the nation has fallen victim to a national strategy that places far greater emphasis on incident reporting than the actual detection of malicious code and cyber weapons before they are used. Making matters worse, programs to enhance the security of vulnerable sectors and their information technology, as well as recovering from a major cyber attack are largely inadequate or non-existent. Dealing with this overall problem 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. Apart from the issue of malicious code and cyber attack is a related issue of the massive growth in the use and misuse of social media for hostile purposes.[9] Here information operations and use of disinformation has become a major national security concern and worth of far greater analytical effort by the Intelligence Community than appears to be the case at present.

Major Cyber Threats: The Cyber Axis of Evil

The United States and its allies face specific and growing threats from four hostile states, a "Cyber Axis of Evil" — China, Russia, Iran, and North Korea. Recent studies detail their investment in cyber capabilities ranging from cyber espionage to hostile cyber attacks scalable to large-scale cyber warfare.[10] High level policy guidance from the White House, the Intelligence

---

[10] 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 Power and Military-Civil Fusion* (New York: Margin Research, February 2023), and 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).

[10] For an early analysis of this problem for NSA, see *Collection and Analysis of Social Awareness Streams (SAS)* (February 2011).

[10] 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 Power and Military-Civil Fusion* (New York: Margin Research, February 2023), and Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner, *Russia's Cyber Operations: A Threat to American*

Community, the Defense Department, and others identify this set of threats but fail to provide any specific programmatic approach to dealing with them.[11]

National policy and current budgets, in the tens of billions, face the kinetic threat posed by nations such as China and Russia stockpiling nuclear weapons and their delivery systems. At the same time these same hostile powers are also creating and stockpiling cyber weapons, such as zero day exploits and others, which can be used in a non-kinetic attack or in conjunction with a kinetic attack with disastrous consequences.

Investments in dealing with this threat and set of weapons is beneath trivial. Also of major concern is also the fact that cyber attacks can "scale" from lower the nation is investing heavily in the possibility of attacks that are very unlikely to happen, and giving short shrift to attacks that very well might happen. This is not a sound strategy.

Collection and Analysis of Hostile Cyber Operations

Realistic programs are urgently needed that promise to be more effective and useful in this technological environment than is currently the case. Notwithstanding a late start, collection against international Internet traffic has become a mainstream activity for the Intelligence Community.[12] The actual work has been handed off to a series of successor groups and offices that have done an increasingly respectable job of collecting and analyzing the traffic for some purposes. By and large this has all been at a macro level and does little to support the growing threat from hostile cyber operations.

Malicious cyber activity, ranging from malware to espionage to cyber warfare activities requires a far different approach than the bulk collection and analysis of Internet traffic. Collection needs to focus on specific software code artifacts of various types. Some come in the form of "patches" to widely used operating systems, such as Linux, and others are "zero day" exploits or similar cyber weapons.[13]

Two DARPA-funded pilot projects show the way. Created under the SocialCyber initiative, the OVERWATCH database contains the largest accessible collection of potentially malicious code

---

National Security (New York: Margin Research, 2023). Work on Iranian cyber operations is still in progress. Analysis of the DPRK cyber operations problem remains unfunded.

[11] See, for example, The White House, *National Cybersecurity Strategy* (March 2023). In recent Congressional testimony FBI Director Christopher Wray noted that Chinese manpower in the cyber area outmatched the U.S. by 50 to 1. At the same time he noted that the U.S. could deal with this threat with "traditional law enforcement methods" which is simply nonsensical. The FBI has no ability to stop bank robberies before they happen, and there is no reason to believe they can stop cyber attacks in advance either.

[12] The 9/11 terrorist attacks on the U.S. provided great impetus to the Intelligence Community in dealing with new communications technologies that had been left on a "back burner" or previously ignored.

[13] A pioneering set of developmental projects were undertaken under the DARPA SocialCyber program, were highly successful but are no longer being funded. Transition of these AI tools to operating agencies with the Intelligence Community has yet to take place.

and artifacts from the four nations identified in the cyber "axis of evil." At the end of 2023, this database contained over 500GB of such data. As far as is known, this database is unique.

Reviewing and analyzing this massive amount of data in OVERWATCH cannot be done manually. The REAGENT AI tool set, developed in parallel to OVERWATCH, searches the data on an ongoing basis to identify potentially malicious code and specific individuals responsible for code artifacts.

Analysis of Hostile Cyber Actors and Their Institutions

Enhancing these technological advances are the use of analysts with native-level language skills, including Chinese, Russian and Farsi. The analysts look at data related to individual actors and their relationship to various institutions including government, intelligence services, and military establishments.[14] This integrated approach is essential to understanding, not only the specific threats, but also their place in an overall security strategy.

This effort followed the successful Intelligence Community approach during the Cold War to understand Soviet weapons systems and individuals and organizations involved in developing them. It is far easier today to obtain data on the individuals involved in China and Russia, for example, from their appearance in code development and on social media.

China, for example, engages in an integrated program for the development of malicious software. China recruits skilled personnel, organizes their cyber operations, and integrates these activities in support of their military and intelligence services. The PRC accomplishes much of this through the Military-Civil Fusion (MCF) program that has enabled China to expand its cyber capabilities in both the commercial sphere as well as in intelligence, espionage, deception, and cyber warfare.

In developing the MCF program, China looked at U.S. examples to understand how the defense and private sector could be effectively integrated in the technology space to meet critical national requirements. China did not copy so much as learned from the United States and crafted its own structure for integrating universities, commercial firms, and defense and intelligence agencies as well as develop individuals with high-level, particular, skills. The result is highly effective cyber tools and operations.

Russia and Iran have not followed the Chinese MCF model exactly. Each has developed its own method for recruitment and organization of cyber talent. The Russian government uses a network including government cyber units, principally in the Federal Security Service (FSB), Foreign Intelligence Service (SVR), and military intelligence agency (GRU), to conduct cyber operations. It also uses cybercriminals recruited by the government as well as hackers approaching government-created front companies.[15]

---

[14] See *China's Cyber Power and Military-Civil Fusion, op. cit.*

[15] The Russian government also leverages hackers with mafia-style familial connections to the security services, encourages patriotic hackers, weaponizes private military companies (PMCs), and uses private-sector conferences and gatherings to recruit talent. See *Russia's Cyber Operations, op. cit.*

Less is currently know about the specifics of hostile code development in Iran, although some study effort is currently under way.[16] Collection against potentially malicious code being developed by Iran and some contract coders supporting Iran is now being included in the OVERWATCH database and being examined to tie to specific individuals and their organizations or sponsors in that hostile nations.

The Need for a Robust Cyber Offense

As in any other national security area it is not enough to detect hostile attacks and recover from any damage inflicted. A corresponding offensive capability is essential to deter cyber attack. For some years, various strategy documents have included this point.[17] At the same time, actual operational capabilities appear to fall far short of high-level policy pronouncements. While DoD did in fact recognize cyber as a new domain in warfighting and formed the U.S. Cyber Command (CYBERCOM) as well as related units in each of the military services, much more can and should be done.

Under Title 10 and Title 50 the responsibility for building a robust cyber offense lies with the Intelligence Community and its colleagues in CYBERCOM. Once again existing capabilities and the ability to generate the needed level of response capability appear to be overly limited by management, insufficient funding, and difficulties in attracting talent internally due to pay and security considerations. CYBERCOM has been slow to outsource this requirement to qualified firms that have needed skills that might support such an effort.[18]

Building a Cyber Workforce

America requires a workforce capable of understanding and confronting risks and threats arising from the cyber domain. Some estimate the national requirement in this area is for some 350,000 people, a number that will continue to grow. Young people will not seek undergraduate and graduate education in this area without funding. Just as America responded to the 1960s challenge of the "space race," it is essential that the nation strongly support education in computer science and related areas.[19]

---

[16] *Iranian Cyber Operations Threat Analysis and Response* (New York: Margin Research, February 2024). See also Emerson T. Booking and Suzanne Kianpour, *Iranian Digital Influence Efforts* (Washington: Atlantic Council, 2020).

[17] See, for example, *Department of Defense, 2018 National Defense Strategy,* (January 2018), p. 6. Subsequent policy documents largely repeat this language.

[18] There are some legal concerns here about what can be done by contractors as opposed to actual government and assigned military personnel.

[19] The creation of ARPA (later renamed DARPA) was itself one element of the national response to the "space race" and the technology challenge of the time posed by developments in the Soviet Union. See, for example, Sharon Weinberger, *The Imagineers of War: The Untold Story of DARPA, The Pentagon Agency that Changed the World,* (New York: Alfred Knopf, 2017), and George A. Kistiakowsky, *A Scientist at the White House* (Cambridge: Harvard University Press, 1976). It is essential that America promote education in computer science and related areas to meet the job requirements in the cyber area. An initiative similar to the National Defense Education Act (NDEA) could be useful in meeting this need.

Looking to the Future

Apart from meeting the current threat in the cybersecurity area it is essential that attention also be given to how the threat is evolving, both in terms of the technologies as well as how they will be employed by hostile actors. Both areas are highly dynamic and present a significant intelligence challenge. In the not-too-distant past the area grew quickly from being the domain of bored high school students to one now encompassing espionage and cyber weapons.

In terms of hostile actors, the current focus continues to be on the cyber "axis of evil" – China, Russia, Iran and North Korea. There is no evidence that any of these states will cease further development of cyber activities, and attention needs to be given to how they will be further developed, including the stockpiling of cyber weapons. It is also likely that other potentially hostile states and terrorist organizations will also develop their own capabilities in this area. There are no significant barriers to entry and this has yet to become a serious area for arms control agreements.

It is also the case that the technology base continues to evolve and will also shape the nature of the future threat. Current concern over the impact of artificial intelligence (AI) is just one example of an area that was of limited interest only a few years ago. Others, such as quantum computing and new methods of software development will shape the threat the intelligence community and the Defense Department will be facing in the years to come.

A Call to Action

Even though various operational programs remain classified and compartmented, the overall problem remains in public view. Several top-level organizational efforts to solve the problem, such as the creation of a White House Office of the National Cyber Director, this office has a large staff that thus far has accomplished close to nothing.[20] For its part the Office of the Director of National Intelligence (ODNI) has more specific responsibility to oversee activities in the cyber area but has thus far been unable to bring the operating agencies to implement the needed program, or to ensure that they are adequately funded.

What is seriously needed is a high level national review of the problem, including the true nature of the threat and what is required in terms of both supporting intelligence as well as operational defensive and offensive programs to meet the challenge. This might be along the lines of the "Team B" approach to major Cold War problems or similar reviews.[21]

While the Defense Department made major progress in recognizing cyber warfare as a legitimate domain of conflict, creating U.S. CYBERCOM and elements within the military services, it has fallen far short in building the operational capabilities to monitor and respond to

[20] The most recent accomplishment of the ONCD was to provide additional funding for Historically Black Colleges and Universities (HBCUs) for more black students to find cyber jobs open in America.

[21] Team B was an analysis commissioned by the (CIA) to analyze threats posed by the Soviet Union at the time due to a 1974 publication that accused the CIA of chronically underestimating Soviet military capability. Years of National Intelligence Estimates (NIE) that were later demonstrated to be very wrong were another motivating factor. Team B was composed of "outside experts" who attempted to counter the arguments of intelligence officials within the CIA.

the evolving threat. Supporting efforts by NSA and CIA also appear to be inadequate compared to the actual nature of this threat. This may in part be due to the government having assigned much of the mission to the Department of Homeland Security and their CISA element which can best be viewed as a major error on the part of successive administrations.

This needs to be changed. Whether this can be accomplished by an executive order, similar to E.O. 12333, or it may need to be done by statute, it needs to be done. Marginal or incremental changes by the existing agencies and offices are not enough.