Better Anticipating and Managing Today's Growing Cyber Risks

Daniel M. Gerstein

> Modern man emerged and began using language 1,400 generations ago. Writing was invented 200 generations ago. Books were first printed 20 generations ago. The invention of the computer occurred less than 2 generations ago.[1]

...And Then Came the Cyber Domain

We live in an increasing cyber enabled world where more of our lives are monitored, assessed, and controlled by forces and decisions that function largely in the background and with little appreciation for the risks that we assume as a result. Absent fundamental rethinking as to how we incorporate Information Age technologies into the fabric of our daily lives, we will increasingly find ourselves reaching a point of no return as more complex technologies such as AI and greater ubiquity of cyber technologies inherent in the Internet of Things (IoT) continue to proliferate in cyberspace. To manage these technologies, we still rely on organizations and processes rooted in the 18th century to confront threats that move across the globe in milliseconds. It is no wonder that we find ourselves in a defensive battle and in a position of great disadvantage.

In considering the current state of cybersecurity, we will do so in its broadest sense. We will consider the computers, networks, technology, and the various means employed for operating in the cyber domain. We will also consider the lower-level components of the Internet that form the basis of cyberspace– these include the computers and Internet of Things (IoT) devices that are an inherent part of the network, packet switching and Internet protocols, cloud computing and the various communications means that comprise the cyber domain and contribute to the increasing attack surface. In looking broadly, we

Dr. Daniel Gerstein, a 1980 West Point graduate, served as the Department of Homeland Security Undersecretary (acting) and Deputy Undersecretary in the Science and Technology Directorate from 2011-2014. He has extensive experience in security and defense and has served in uniform, industry, academia, think tanks and as a senior government civilian. He is currently an Adjunct Professor at American University in Washington, D.C. In uniform he served on four continents during combat, peacekeeping, humanitarian, counterterrorism and homeland security including standing up SOUTHCOM's Theater Network Operations and Security Center following 9/11. He served for more than a decade in the Pentagon in various high-level staff assignments, including having served on the Holbrooke Delegation that negotiated the peace settlement in Bosnia. He is a frequent national security contributor and has published numerous books and articles on national and homeland security issues. His latest book—*Tech Wars: Transforming U.S. Technology Development* (Praeger)—was published in September 2022.

will consider the effects on related technologies such as big data, blockchain, encryption, social media and AI. We will also consider how norms, regulations, and laws contribute to or detract from our cyber lives, and how these issues, within a whole-of-society context that ranges from international and national authorities to each and every citizen, will be affected by and in some cases become part of the cyber domain. As we ponder these concepts, considering effects on society in areas such as loss of privacy, human interactions in cyber space, and sensitive data such as security of personal identifiable information (PII) will also be important.

The purpose in looking so broadly is to understand the overall risks associated with this human created cyber domain. In doing so, we hope to better understand and mitigate such risks in the future.

Our approach to date for dealing with cyber risks has been largely reactive as we install intrusion detection systems and internal network monitoring capabilities to prevent intruders from penetrating our networks and look for anomalous behavior within our networks. At the 2022 DEF CON National Cyber Director Chris Inglis asserted this must change and highlighted that "defense is the new offense," and "the way forward for cybersecurity is defense."[2] With each cyber intrusion, ransomware event, theft of intellectual property or attack on critical infrastructure, we seek to understand how the attack occurred and implement specific changes in the form of software patches, calls for hardware refreshes for obsolete systems or incorporating new procedures to protect our cyber networks.[3]

Despite these efforts, evidence abounds that this approach is inadequate. In the first half of 2021, Accenture found a triple digit increase in cyber-attacks. They further identified five industries that comprised more than 60% of the intrusions, including consumer goods and services, industrial, banking, travel and hospitality and insurance. Not surprisingly, the top three nations

targeted were the US, UK and Australia, and the top threats are ransomware and extortion.

We also have experienced cyber-attacks targeting critical infrastructure that caused serious property damage. Examples include:

- Saudi Aramco attack (2006)
- Attacks that targeted government facilities in Estonia (2007)
- Polish teenager remotely derailing trains (2008)
- Hacker tampering with a hospital ventilation system in a Texas hospital (2011)
- Yahoo cyber-attack that compromised one billion accounts (2013)
- Russian attack against the Ukrainian power grid (2015)
- WannaCry ransomware attack (2017)
- Saudi Arabia's oil refineries attacked (2017)
- JBS attack (2021)
- Colonial Pipeline attack (2021)

These represent only a small but highly visible subset of attacks.[4,5,6]

The continued increase in the number and variety of devices, users, applications, and data have resulted in growing attack surface problems, i.e., the number of points vulnerable to attack continues to grow. Issues are exacerbated by several intertwined and mutually reinforcing trends: the increasing number of IoT sensors and actuators on the network and associated volumes of retained data, evolving sophistication of global supply chains that rely on the Internet, the mass migration of resources to the cloud, and greater remote work activities (which accelerated in the COVID-19 era).[7]

In short, we have applied a serial approach to a massively parallel problem within a complex network, all further complicated by the fundamentals of the cyber domain. At its core, the Internet–the early instantiation of the cyber domain–was created as an information sharing platform with little regard for security. In fact, security was, and still often is, an afterthought or add on feature rather than a coequal part of the Internet. It is further complicated as some 85% of critical infrastructure, to include the Internet and associated infrastructure, reside in the private sector.[8] Even those parts of the cyber domain that are used by government traditionally have portions of their networks that reside in the broader cyber domain. For example, classified networks normally lease communications systems from Internet service providers and employ secure devices to provide security for their networks and data. We also know that a significant percentage of the cyber insecurities occur at the application layer, where human-computer interface occurs and the user operates–by one estimate, 95% of cyber security breaches are caused by human error.[9]

Understanding and Managing Future Cyber Risk

To better manage future cyber risks, we need to better understand them, which requires consideration of two different types of risks. The first are technology risks associated with the development of key cyber enabling technologies. The second set of risks are strategic and occur from lacking the necessary command and control relationships, planning and processes, or failing to take appropriate actions as required to prevent, protect, mitigate, respond, and recover from a cyber event.

The earlier introduction paints a bleak picture of several cyber threats that have materialized in the past and even provides a glimpse of likely future cyber risks. Yet increasing capabilities of Information Age technology could present even greater risks.

To understand how the cyber landscape could evolve, it helps to segment the Internet (and associated World Wide Web or www) into Web 1.0, Web 2.0, and Web 3.0, as described in Table 1 below.[10] Web 1.0 consisted of static pages. Advertisements were banned. Personal users hosted their own web pages on ISP-run websites. Web 2.0 is often called the "participative social web,"[11] which allows for "podcasting, blogging, tagging, curating with RSS, social bookmarking, social networking, social media, and web content voting."[12] It is both enabled by and a product of ubiquitous mobile communications that allow humans to maintain virtually constant contact with the World Wide Web. Web 3.0 would significantly increase Web 2.0 capabilities to allow for "web utilization and interaction, which includes altering the web into a database," thereby optimizing Web 3.0 for "machine conception as opposed to human understanding."[13]

Table 1. Web 1.0, Web 2.0, Web 3.0 Descriptions and Features.

Version	Web 1.0	Web 2.0	Web 3.0
Description	First stage of the World Wide Web evolution	Refers to worldwide websites which highlight user-generated content, usability, and interoperability for end users	Evolution of web utilization and interaction which includes altering the Web into a database
Features	1. Static pages. 2. Content is served from the server's file system. 3. Pages built using Server Side Includes or Common Gateway Interface (CGI). 4. Frames and Tables are used to position and align the elements on a page.	1. Free sorting of information, permits users to retrieve and classify the information collectively. 2. Dynamic content that is responsive to user input. 3. Information flows between the site owner and site users by means of evaluation & online commenting. 4. Developed APIs to allow self-usage, such as by a software application. 5. Web access leads to concern different, from the traditional Internet user base to a wider variety of users.	1. Semantic Web--improves web technologies in demand to create, share and connect content. 2. Artificial Intelligence--uses natural language processing to distinguish information like humans; becomes more intelligent to fulfill the users' requirements. 3. 3D Graphics—3D design is being used widely in websites and services. 4. Connectivity--information is more connected thanks to semantic metadata. 5. Ubiquity--content is accessible by multiple applications, every device is connected to the web, the services can be used everywhere.

This is not to imply that humans will not be important in Web 3.0. Rather, the structure of the data and interactions will enhance machine-to-machine communications and learning. Web 3.0 will transform the World Wide Web with a semantic web that facilitates creating, sharing and connecting content; AI that supports natural language processing and enhanced speed of

action; 3-dimensional graphics that improve both human understandings and computer generated graphics; enhanced connectivity and access to information; and ubiquity with billions of other web-attached devices. In short, Web 3.0 will generate data, decision quality information and enhanced timeliness where humans will be challenged to keep up and machine-to-machine interactions will often dominate.

Today we are at Web 2.0 with some early surfacing features that will likely evolve into Web 3.0. For example, there are AI uses on the current web, but in Web 3.0, we should expect that computers would be able to differentiate information as humans do or perhaps even more accurately and efficiently depending on the evolution of this technology.

Transitioning from Web 2.0 to Web 3.0 will require technological development along numerous key areas including AI, communications and cybersecurity, big data, the IoT and the Internet of Bodies (IoB),[14] natural language processing, robotics, pattern recognition, machine learning, object recognition speech recognition and statistical learning, to name a few. Indeed, many Information Age technologies must coevolve for this development to proceed toward Web 3.0.

Internet evolution will be fraught with complexities and uncertainties; new approaches to issues such as the curation and storage of personal data; and ultimately a variety of risks from the system to the strategic levels that will require careful management.

DoD's Defense Innovation Board (DIB) proposed AI Principles for the "design, development, and deployment of AI for both combat and non-combat purposes,"[15] and provides a useful point of departure for considering the implications of managing future cyber technology development risks. The stated goal is to develop technologies that are: responsible, equitable, traceable, reliable, and governable.

Strategic risks associated with lack of necessary governance relationships, inadequate planning and processes, or failure to take necessary actions also must be carefully considered. The DoD 2018 cyber strategy provided a framework with five reinforcing the lines of effort: build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.[16] However, this document focuses exclusively on military cyber domain considerations.

The more recently published Cyberspace Solarium Commission (CSC) report considers federal civilian and military cyber issues as well as non-governmental cyber concerns, and hence is more encompassing. The CSC was established in the National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the US in cyberspace against cyber attacks of significant consequences."[17] The bipartisan commission released its July 2020 report that contained over 80 recommendations organized into six pillars. The document was intended to serve as a road map for Congressional legislation to be developed (See Table 2).

The CSC report highlights shortfalls in organizational structures and coordination between federal and non-federal government entities, industry, academia, non-profits and international partners and stakeholders, and recognizes the importance of international norms and robust signaling and deterrence capabilities. It also stresses the importance of preparedness and response capabilities (including resilience) should deterrence fail.

Table 2. Cyberspace Solarium Commission Report Findings (July 2020)

The Cyberspace Solarium Commission report consists of over 80 recommendations organized into 6 pillars:

1. ***Reform the U.S. Government's Structure and Organization for Cyberspace.***
   – While cyberspace has transformed the American economy and society, the government has not kept up.
2. ***Strengthen Norms and Non-Military Tools.***
   – A system of norms, built through international engagement and cooperation, promotes responsible behavior and dissuades adversaries from using cyber operations to undermine American interests.
3. ***Promote National Resilience.***
   – Resilience, the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or otherwise shape U.S. behavior, is key to denying adversaries the benefits of their operations and reducing confidence in their ability to achieve their strategic ends.
4. ***Reshape the Cyber Ecosystem.***
   – Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries' activities.
5. ***Operationalize Cybersecurity Collaboration with the Private Sector.***
   – Unlike in other physical domains, in cyberspace the government is often not the primary actor.
6. ***Preserve and Employ the Military Instrument of National Power.***
   – Future crises and conflicts will almost certainly contain a cyber component. In this environment, the United States must defend forward to limit malign adversary behavior below the level of armed attack, deter conflict, and, if necessary, prevail employing the full spectrum of its capabilities.

Assessing Future Cyber Risks

Assessing the future cyber risk will require us to examine both the technology development principles identified by the DIB and strategic risks identified by the CSC. Many technology risks will be illuminated by the DoD (DIB) proposed principles for "design, development, and deployment of AI." These stated goals (i.e., responsible, equitable, traceable, reliable and governable) will be key as we develop technologies and transition from Web 2.0 to the more AI-based Web 3.0.

Responsible requires that humans exercise judgment in developing, deploying, using, and arriving at outcomes. Accomplishing this requires humans to embed structures and processes that directly account for and retain human control in the algorithms that enable the functionality of the cyber domain. It also requires keen human judgments in decision-making, a point important to consider more deeply.

Increasingly, we will see cases where computer-developed capabilities far exceed the speed, efficiency, and effectiveness of human-developed capabilities. To reduce the risks associated with these machine-created systems, humans, before embracing these new capabilities, need mechanisms in place that safely validate the new designs. As an example, consider development of an aerial drone chassis using AI technologies. By adding the goals of the design—i.e., the parameters of the system to be developed–the computer can optimize the platform design.[18] But beyond development of the drone, the system needs to be validated through a mix of tests and simulations conducted in both the virtual and real worlds.

While this sounds sensible, there are unfortunate examples where such appropriate care was not taken. Consider the Boeing aircraft company issues with the 737 Max aircraft Maneuvering Characteristics Augmentation System (MCAS) flight control, which through the combination of system design failures, inadequate training of pilots, and failure to alert the airlines to the incorporation of this technology resulted in the death of hundreds of people in two separate crashes.[19] This incident highlights two other painful lessons. The first is the fragility of human computer interfaces. For humans and computers to interoperate in systems, key information flows can become life-and-death essential to safe operation. Second, even if it is an automated system that fails, humans remain responsible for the outcomes. In this case, Boeing was found to have created an unsafe system that required modification and recertification for flight, and otherwise posed liability and crash-related lawsuits.

As capabilities become more complex, cyber community stakeholders will be challenged to establish responsibility without a deliberate focus on this area. As the hardware, software and processes (and algorithms) become less transparent, allocating responsibilities will become even more challenging, as discussed below under "traceability."

Equity in cyberspace requires concrete measures to avoid bias in developing and deploying cyber-related systems, and to mitigate biases injected by cyber platform users (e.g., social media and deepfakes), to include both deliberate and unintended biases. For example, search engine developers often accord their parent company advantages such as responses to be loaded first and hence more likely to be viewed. In today's Web 2.0, the greater number of clicks would result in advertisers paying more to preferred sites.

Unintended bias may manifest in search engines that reflect racist, sexist, or anti-Semitic attitudes as well. For example, Google discovered shortly after going public in 2004 that searching the term "Jew" returned hits on anti-Semitic websites.[20] The very concept of search engine usage creates these kinds of unintended issues. Search history is often targeted to identify other websites that might align with a person's values, thereby opening the door to sites or topic areas perceived to be aligned. This can improve user' experience, but also can lead to reinforcing biased behaviors through online content.[21] This was recently seen as a contributing cause of COVID-19 vaccine hesitancy.[22]

Facial recognition algorithms have come under scrutiny for their poor performance for certain demographic groups. One study points to "divergent error rates across demographic groups, with the poorest accuracy consistently found for those who are female, Black, and 18-30 years old."[23] In this 2018 "Gender Shades" project, three facial recognition algorithms were compared for different demographic categories. The findings indicated, "All three algorithms performed the worst on darker-skinned females, with error rates up to 34% higher than for lighter-skinned males."[24] With such a glaring gap in accuracy across demographic categories, it virtually assures low acceptability of the technology, particularly among disenfranchised groups.

Some of these issues of equity relate to the how the original research was conducted. Initial facial recognition data disproportionately used homogeneous white male populations, making facial recognition outside this grouping far less accurate. To address this issue, the facial recognition algorithms need to be trained on more "diverse and representative datasets." In collecting data, adjusting camera settings to better "capture people with darker skin tones" has been found to be useful. Finally, routinely assessing performance through regular "ethical auditing" should be incorporated to render facial recognition systems more accurate and hence reliable.[25]

Traceability requires understanding the technology, development processes, and methods of operational systems, including having transparent and auditable methodologies, data sources, and design procedures and documentation.[26] It implies having a direct line of sight through the lifecycle of the technology and across all its component parts. It is important to understand that a failure across any part of the system can result in catastrophic failure of the entire system in an operational setting.

Traceability requires validation and verification of the system and its component parts in both test and operational environments. Validation pertains to whether the system functions as intended, according to the customers' requirements. It answers the question, "Am I building the right product," and includes customer acceptance and usability testing. Verification ensures that the product adheres to specifications, and is conducted while the product is still under development, and can be done on individual modules or the complete system. It answers the question, "Am I building the product right," and includes unit, integration, and automated testing. Both validation and verification make use of regression, system, and Beta testing.[27] And, as with our previous facial recognition example, shortfalls in systems development and inadequately robust data hinders traceability of the results.

Self-driving cars illustrate yet another interesting traceability challenge. Self-driving cars depend on three autonomous systems that must function synchronously. The perception module uses cameras, radar, and LiDAR to identify objects in a car's vicinity. The prediction module forecasts the movements of these near neighbors. Finally, the decision module sets the driving policy and acts based on the inputs received from the other two modules. Despite inherent safety benefits of autonomous vehicles and millions of miles in real-world testing, technology concerns persist, and center around two issues: the legal implications of autonomous vehicle accidents and software traceability. To this second point, understanding how changes made affect vehicle functionality is imperative for traceability–ensuring that a digital thread exists that will confirm the software as well and thereby allow for auditing is essential.[28]

Traceability is also central to any debate about lethal autonomous weapon systems (LAWS). Autonomous systems are already employed for defensive purposes–such as the Phalanx close in anti-missile gun on several Navy ships and Israel's Iron Dome counter mortar system that the US has also employed in Iraq and Afghanistan, yet the offensive use of LAWS continues to

be debated. The concern arises in the case of an allegedly unjust killing where one philosopher argues "that the autonomy of LAWS makes it impossible to hold anyone accountable for illegitimate killings they commit."[29] Who should be held responsible if the robot acted autonomously? This creates what some have called a "responsibility gap" that some find "morally objectionable and legally infeasible."[30]

A software bill of materials (SBOM) has become a "key building block in software security and software supply chain risk management." SBOM guidance for developing software increases the transparency of products developed, information on SBOM tools that support creators and vendors in classifying their products, and summaries of formats and standards for software development. In short, SBOM enhance the traceability of the software.[31]

Reliability requires an "explicit, well-defined domain of use, and the safety, security, and robustness of such systems should be tested and assured across their entire life cycle within that domain of use."[32] Reliability overlaps with validation and verification discussed under traceability above. Testing at all stages of development should continue throughout a system's lifecycle, from basic and applied research to early-stage development, and throughout fielding and use in operational environments.

It would be comforting to observe the great benefits experienced to date from the cyber domain and the invaluable uses of these technologies. In the same breath, one could confirm explosive growth of the cyber economy with great benefit to those able to incorporate the technology. All true, but the cyber domain also has contributed to instability, both within the US and indeed, worldwide. We have seen conclusive evidence of devastating physical and other damage to critical infrastructure, to say nothing of the adverse effects of tainted information and sources of news which have become no longer trustworthy.

Reliability shortfalls in our hardware, software, networks, and data storage capacity often contribute to the initial breach and the severity of the intrusion. The Office of Personnel Management (OPM) data breach–characterized as the most significant breach of sensitive personnel data to have ever occurred–began in November 2013, but was not discovered until June of 2015.[33] OPM's system was breached with over 20 million SF-86 security clearance adjudication packages exfiltrated over an 18 month period. While China was identified as the perpetrator, even the post-breach period demonstrated a lack of system reliability and resilience coupled with shortfalls in preparedness, response and resilience.[34] This data breach highlighted numerous deficiencies and insecurities ranging from procedural issues and inadequate cyber hygiene to antiquated systems and obsolete methods for storage of sensitive data. The breach was not discovered until government software (Continuous Diagnostics and Monitoring (CDM)) was being installed. The breach highlighted the challenges that "smaller-sized, medium-sized agencies that didn't consider themselves to be [at] such a threat to cyberactivity from data thieves, that they also have this potential [negative] publicity associated with becoming a target and becoming a victim."[35]

More recent cyber breaches such as the Colonial Pipeline ransomware and log4j software vulnerability continue to demonstrate the inadequate security of the Internet and its associated components. To put a fine point on these issues, they have exposed the lack of reliability in our systems. As with other such cyber incidents, the Colonial attack exposed an important human dimension which contributed to the breach as the attackers gained access to the network through an "exposed password for a VPN [virtual private network]."[36] Despite planning, exercises and even simulations of attacks against U.S. infrastructure, we collectively–Colonial, the critical infrastructure sector and nationally–were not prepared when a criminal extortion ring gained control of corporate data and held it for ransom. Colonial Pipeline was left to conclude that their supposed "impermeable wall of protections was easily breached."[37]

The discovery of the log4j vulnerability should give us great cause for concern. U.S. Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly, identified the log4j vulnerability as "the most serious vulnerability I have seen in my decades-long career."[38] Log4j is free "code that helps software applications keep track of their past activities."[39] The vulnerability is created if a line of malicious code is inserted into the software that would allow "bad actors [to] grab control of servers that are running log4j."[40] The ubiquity of this code is cause for great concern. Perhaps more concerning is that the code, and hence this zero-day vulnerability, was in use for years before being discovered in 2021. What does this say about our software assurance capabilities and how many potentially catastrophic log4j-like vulnerabilities are in the offing?

A final note on reliability is in order here. Numerous hacks, attacks, breaches, and insecurities have resulted from legacy systems running obsolete hardware and software components that are generations past their technological prime. Despite security patches and efforts to improve user awareness and procedures, there is only so much that can be done. Eventually obsolete equipment must be replaced. This challenge is magnified as most of the cyberinfrastructure, some 85% of all US-based cyberinfrastructure, is in the private sector and hence requires private sector investments to be made.[41]

By way of a postscript on reliability, Microsoft's report, *Defending Ukraine: Early Lessons from the Cyber War*, illustrates that cyber lessons regarding reliability are being learned in real time. For example, having dispersed and distributed digital operations within and outside of a nation's national borders is critical. A combination of threat intelligence and endpoint protection have mitigated some of the threats that had the potential for devastating consequences. Having a coordinated and comprehensive cyber strategy that includes defenses against "destructive cyberattacks, espionage and influence operations" is essential. As with any conflict, both sides can adapt. This has been reinforced in the Russia-Ukraine war as Russia has increased its network penetration and espionage activities, targeting both Ukraine and allied governments supporting Ukraine.[42] The message is that regardless of the preparations and response capabilities that have been developed, adapting in real time to threats and vulnerabilities is essential to stay ahead of adversaries.

Governable connotes a system "designed and engineered to fulfill their intended function while possessing the ability to detect and avoid unintended harm or disruption and disengage or deactivate deployed systems that demonstrate unintended escalatory or other behavior." Governability significantly overlaps with reliability. Certainly with 85% of critical infrastructure held privately, governance is a huge challenge. Technical challenges also pose governance hurdles—the log4j vulnerability is but one example, which brings to mind the adage, "if you've seen one cyber-attack, you've seen one cyber-attack." This makes governance in cyberspace increasingly more challenging.

Recent experiences illustrate that the magnitude of the intrusion or attack also contributes to the challenges of governing cyberspace. The SolarWinds breach penetrated a number of US government agencies—including the Treasury and Commerce Departments, and unconfirmed reports of the Department of Defense, NASA and the White House—and compromised hundreds of organizations worldwide.[43] *Cybercrime Magazine* estimates that the world will lose $10.5 trillion annually to cybercrime by 2025. Highlighting the implications of this risk, the source identifies cybercrime as "the greatest transfer of economic wealth in history."[44] The numbers illustrate just how pervasive the problem is becoming.

The news is no better for the effects on social media which has been implicated in a variety of ills including manipulated elections, inciting violence, facilitating cyber bullying and cyber abuse, and proliferating offensive and illegal content. After revelations of social media's—in particular Facebook (now Meta)–influence over the 2016 elections, the company announced that it barred all political advertisements the week before the 2020 elections.[45] According to a Pew Research survey, "Many users see social media as an especially negative venue for political discussions," despite its growing user base and continued use for this purpose.[46]

So how should we think about issues of cyber governance? Several key shortfalls underlie the demonstrated inability to govern cyberspace.

First, the tools to appropriately govern cyberspace are lacking. The only true governance on the Internet today are the technical specifications that allow the Internet to function. No one or no single organization is in charge of the Internet. Cyberspace grew up as an organic domain and has continued to evolve to its current state. The Internet was not centrally planned and has truly been built from the ground up. As new concepts and capabilities are incorporated into the Internet, the evolution continues. The horizontal and vertical growth of the Internet tech companies demonstrates this evolution. This puts leaders of large tech firms in the position of governance over large swaths of the Internet which often leads to conflicts of interest, placing shareholder value and public safety interests at odds.[47]

Second, the Internet lacks the ability to sense in real-time when anomalous and potentially dangerous activities are occurring. Here the Internet should be considered in its broadest sense and include governments, industry and the private sector, and individual users. Capabilities

are incorporated into the Internet before they are fully understood, with guardrails installed, often after the fact, to address potential vulnerabilities.

Third, we rely on users for too much sophistication. One assessment focusing on the human factor in IT [information technology] security, observes that over half of the companies "believe they are at risk from within" from user carelessness or lack of knowledge.[48] This concern was even more pronounced for smaller corporations. Even for personal use, an expectation of sophistication is inherent. Individual users are expected to understand the threats and vulnerabilities, replace obsolete systems, and routinely patch their systems. These expectations continue despite estimates that "95% of cybersecurity breaches are a result of human error, only 5% of companies' folders are properly protected, only 16% of executives say their organizations are well prepared to deal with cyber risk, and over 77% of organizations do not have a cyber security incident response plan."[49]

STRATEGIC CYBER RISKS

In the previous section we discussed technology development principles for cyberspace technologies. Here we will briefly consider the strategic implications associated with cyberspace. For this purpose, the Cyberspace Solarium Commission provides a useful point of departure. Unlike in the previous section's focus on the individual development principles, reference to the CSC is to remind the reader that the cyber domain is global and overlays the other natural domains (i.e., land, maritime, air, and space).

We must remain mindful that the Solarium Commission's six pillars and 80 recommendations cannot apply solely within the US. Optimally, they must apply to the entire international cyberspace domain. As an example, the first CSC pillar calls for reforming the US structure and organization for cyberspace. That structure must also fit within international structures and organizations. For example, the US cyber structures and organizations should support economic activities, account for societal norms, and also be aligned with international laws and regulations.

Several Solarium Commission recommendations pertain to building capacity to improve security, strengthen norms, and enhance resilience to withstand and recover. These activities should be undertaken with a keen eye toward the five technology development risks discussed in the previous section—cyber domain technologies developed must be: responsible, equitable, traceable, reliable, and governable.

Having internationally accepted cyber domain "rules of the road" going forward is vitally important. Unless these rules effectively police against behavior that is irresponsible, inequitable, untraceable, unreliable or ungovernable, it is difficult to envision how the Internet can continue to serve US interests and values.

As the CSC emphasizes, all stakeholders must be considered and represented, and governments at all levels must meaningfully participate in establishing laws, norms, and regulations. Industry and academia bring the greatest technical knowledge and therefore must be represented when solutions are needed. Private citizens must have input as they will increasingly find the cyberspace dominating important aspects of their lives.

CONCLUDING THOUGHTS

Ideally, transition from Web 2.0 to Web 3.0 should not occur until the technology development and strategic cyber risks have been carefully analyzed and addressed. However, logic may not govern transition to Web 3.0. Already we are witnessing the rapid incorporation of IoT (and soon IoB) devices, wearables, machine learning and AI technologies long before most even realize the rapid transition is occurring.

Moving to Web 3.0–which will rely on greater use of machine-to-machine communications and less human intervention–should evolve deliberatively, and only after adequate assessment and mitigation of risks are fully incorporated into the future cyber domain. Here the DoD (DIB) principles provide a useful framework for understanding these risks and developing approaches to mitigate concerns. In concert greater progress must also be made to address strategic cyber risks.

Continuing to advance before the range of threats, vulnerabilities, and consequences inherent in the future cyber risks of Web 3.0 are fully analyzed and mitigated at each step of our progressive evolution towards Web 3.0 not only would be wrong; it also would be foolhardy.

NOTES

1. Tim Chao, Tuan Pham and Mikhail Seregine, "The Dangers of Technological Progress," Stanford University, https://cs.stanford.edu/people/eroberts/cs201/projects/1999-00/technology-dangers/issues.html, accessed December 6, 2018.
2. Kirsten Errick, "White House Cyber Director: 'Defense is the New Offense' for Cyber," Nextgov, August 14, 2022, https://www.nextgov.com/cybersecurity/2022/08/white-house-cyber-director-defense-new-offense-cyber/375822/.
3. "Triple digit increase in cyberattacks: What next?" Accenture, August 4, 2021, https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks.
4. "6 Cyber Attacks that Caused Property Damage," The ALS Group, March 14, 2017. https://info.thealsgroup.com/blog/cyber-attacks-property-damage.
5. "When Cyber threats get Physical," Clyde and Co, May 17, 2021, https://www.clydeco.com/en/insights/2021/05/when-cyber-threats-get-physical.
6. Sama Al-Kurdi, "The 10 Biggest Cyber Attacks In History," *Albawaba*, June 26, 2021, https://www.albawaba.com/business/10-biggest-cyber-attacks-history.
7. "are the jbs and colonial attacks just the beginning?" Silent Breach, https://silentbreach.com/BlogArticles/are-the-jbs-and-colonial-attacks-just-the-beginning/.
8. Paul Rosenzweig "Is It Really 85 Percent?" *Lawfare*, May 11, 2021, https://www.lawfareblog.com/it-really-85-percent.
9. Rob Sobers, "134 Cybersecurity Statistics and Trends for 2021," Varonis, March 16, 2021, https://www.varonis.com/blog/cybersecurity-statistics/.
10. "The Internet is a global network of networks while the Web, also referred formally as World Wide Web (www) is a collection of information that is accessed via the Internet," What's difference between the Internet and the Web? GeeksforGeeks. Last updated November 3, 2021, https://www.geeksforgeeks.org/whats-difference-internet-web/#:~:text=The%20Internet%20is%20a%20global,on%20top%20of%20that%20infrastructure.
11. Ibid.
12. Ibid.
13. Ibid.
14. Bernard Marr, "What Is The Internet Of Bodies? And How Is It Changing Our World?" *Forbes*, December 6, 2019, https://www.forbes.com/sites/bernardmarr/2019/12/06/what-is-the-internet-of-bodies-and-how-is-it-changing-our-world/?sh=421e2dbf68b7
15. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense by the Defense Innovation Board (Undated), https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF, While this document pertains specifically to ethical use of AI, the categories also related directly to examining the risks.
16. Summary: Department of Defense cyber strategy 2018, U.S. Department of Defense, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
17. Cyberspace Solarium Commission (CSC), https://www.solarium.gov/.
18. "Drone design artificial intelligence," TEDx, March 1, 2017, https://www.youtube.com/watch?v=odHC-gxJhG4.
19. Darryl Campbell, Redline: The many human errors that brought down the Boeing 737 Max," The Verge, May 2, 2019, https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa.
20. Edward Tenner, "Search Engines May Seem All-Knowing, But They're Not. Here's How to Get More Trustworthy Results" *Time*, June 26, 2018, https://time.com/5318918/search-results-engine-google-bias-trusted-sources/
21. Bias in the machine: Internet algorithms reinforce harmful stereotypes," Princeton University, Department of Computer Science, November 22, 2016, https://www.cs.princeton.edu/news/bias-machine-internet-algorithms-reinforce-harmful-stereotypes.
22. Matthew Daniel, "Fake news, politics, and behavioral biases: A perfect storm for vaccine hesitancy," BenefitsPRO, January 6, 2022, https://www.benefitspro.com/2022/01/06/fake-news-politics-and-behavioral-biases-a-perfect-storm-for-vaccine-hesitancy/?slreturn=20220715112223.
23. Alex Najibi, "Racial Discrimination in Face Recognition Technology," Harvard University: Science in the News. October 24, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/
24. Ibid.
25. Ibid.

NOTES

26. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense by the Defense Innovation Board (Undated), https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.
27. "Verification vs Validation: Do You know the Difference?" Plutora, November 23, 2020, https://www.plutora.com/blog/verification-vs-validation.
28. Patrick Londa, "Autonomous Vehicles Pose an Unprecedented Software Challenge," *Design News*, August 28, 2018, https://www.designnews.com/automotive/autonomous-vehicles-pose-unprecedented-software-challenge.
29. Matthew Anzarouth, "Robots that Kill: The Case for Banning Lethal Autonomous Weapon Systems," *Harvard Political Review*, December 2, 2021, https://harvardpolitics.com/robots-that-kill-the-case-for-banning-lethal-autonomous-weapon-systems/.
30. Ibid.
31. Software Bill of Materials, Department of Commerce, National Telecommunications and Information Administration, Accessed March 7, 2022. https://ntia.gov/SBOM.
32. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense by the Defense Innovation Board, October 31, 2019, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.
33. Michael Adams, "Why the OPM Hack Is Far Worse Than You Imagine," *Lawfare,* Friday, March 11, 2016, https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.
34. Ian Smith, "Bolton Confirms China was Behind OPM Data Breaches." FedSmith. September 21, 2018, https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/.
35. Brian Naylor, "One Year After OPM Data Breach, What Has The Government Learned? *NPR*, June 6, 2016, https://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned.
36. Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know." Tech Target: WhatIs.com, April 26, 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=What%20was%20the%20root%20cause,Homeland%20Security%20on%20June%208.
37. David E. Sanger and Nicole Perlroth, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity," *The New York Times*, May 14, 2021, updated June 8, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.
38. Tatum Hunter and Gerrit De Vynck, "The 'most serious' security breach ever is unfolding right now. Here's what you need to know." The Washington Post, December 20, 2021, updated December 20, 2021, https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/
39. Ibid.
40. Ibid.
41. Paul Rosenzweig, "Is It Really 85 Percent?" *Lawfare*, May 11, 2021, https://www.lawfareblog.com/it-really-85-percent.
42. Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.
43. "are the jbs and colonial attacks just the beginning?" Silent Breach, https://silentbreach.com/BlogArticles/are-the-jbs-and-colonial-attacks-just-the-beginning/.
44. Steven Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine,* November 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
45. Michael Baldassaro and David Carroll, "It's time for Congress to regulate political advertising on social media," *The Hill*, October 7, 2020, It's time for Congress to regulate political advertising on social media | TheHill.
46. Lee Rainie, "Americans' complicated feelings about social media in an era of privacy concerns," Pew Research Center, March 27, 2018, How Americans feel about social media and privacy | Pew Research Center
47. Craig Timberg, "Net of Insecurity: A Flaw in the Design." *The Washington Post*, May 30, 2015. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.
48. "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," *Kaspersky Daily*, https://www.kaspersky.com/blog/the-human-factor-in-it-security/.
49. "15 Cybersecurity Statistics in 2021," TitanFil, https://www.titanfile.com/blog/15-important-cybersecurity-statistics-in-2021/.