# Defending U.S. National Security Against Cyber Threats

**Surya Prakash Reddy Pakanati, Tye Lee, Olafuyi Olajide, Dee Nickerson, Olafuyi Basiru, Shamice Jackson**

DOI: 10.29322/IJSRP.16.04.2026.p17223
https://dx.doi.org/10.29322/IJSRP.16.04.2026.p17223

Paper Received Date: 16th March 2026
Paper Acceptance Date: 14th April 2026
Paper Publication Date: 22nd April 2026

***Abstract-*** Advancements in digital technology have ushered the country into a new frontier. Government agencies, military and defense systems, financial systems, businesses, and national infrastructure are rapidly relying on internet-connected computer systems. As more of America's national security apparatus moves into cyberspace, the nation is met with expanding threats from foreign nations, cyber criminals, terrorists, and insiders. Cyber threats pose national security risks to Americans by threatening to undermine the delivery of essential services, steal government secrets, inflict financial harm to the economy, and erode democratic processes. This research paper seeks to understand cyber threats to U continuity of national security and the defense strategies employed to combat them. Topics covered include the threat landscape, critical infrastructure vulnerabilities, how adversaries are capitalizing on emerging technologies like artificial intelligence, and how the U.S. government is approaching cyber defense policy through public-private partnerships, a national cybersecurity strategy, and cybersecurity technology. Through this research it was found that defending America's national security interests in cyberspace requires a unified and collaborative approach to cybersecurity incorporating government leadership, private sector alignment, technology solutions, and international partnerships.

***Index Terms***- Cyber defense, Cybersecurity policy, National security, Threat intelligence.

## I. Introduction

In today's technological advancements information technology (IT) systems remain integrated into every aspect of national security, including the economy, military defense, societal functioning, and critical infrastructure. This cybersecurity environment brings new opportunities as well as vulnerabilities that can be exploited by a variety of threat actors. Today, cyber threats are not only carried out by independent hackers but also nation-states, organized criminals, and other non-state actors interested in stealing private data or disrupting critical operations. The purpose of this paper is to research cybersecurity threats that affect U.S national security and discover measures to prevent such attacks.

Cyberattacks on national security can range from breaches of classified data to ransomware deployment, spying, and disruption to critical infrastructure systems. Current cybersecurity reports show that cyber threats are likely to come from foreign government groups. Cybersecurity Intelligence states that "China, Russia, Iran, and North Korea frequently target U.S. Government agencies, Defense Industrial Base contractors, and public/private organizations through cyber espionage and compromise campaigns" (Rid and Buchanan, 2015). Foreign groups can target electric grids, financial networks, hospital systems, and many other structures that pose serious threats to national security if compromised. These attacks have been on the rise over the past few years causing urgent need to develop a more secure cybersecurity environment.

Cyber threats often pose a unique challenge in terms of response as they are usually asymmetrical. Many cyber operations can be deniable and relatively cheap to conduct which makes it challenging to respond to an attack if the culprit is not identified. Cyber threats can also occur at any time without any regard to time zones and often target both public and private sector systems. An example of a cybersecurity attack affecting essential services and posing danger to public safety includes ransomware attacks against hospital systems and townships (Singer and Friedman, 2014). Cybersecurity threats require urgent response once an attack has been identified which leaves systems vulnerable to initial attacks.

The U.S. government has made efforts to provide cybersecurity policies by developing government agencies such as the Cybersecurity and Infrastructure Security Agency. Policies have been set in place to protect critical infrastructure and the general public. Efforts have been made to improve communication between the public and private sector when sharing information about cyber threats. The National Institute of Standards and Technology (NIST) established a cybersecurity framework to help organizations manage cybersecurity risk. Although these efforts have been successful, it is hard to track the implementation of these policies throughout all private sector organizations.

Technology continues to grow and become more intelligent with the use of Artificial Intelligence (AI) and machine learning. Technology can help improve response to cyber threats with AI and machine learning, allowing technology to automate response to cyber incidents. One downside to this is that cyber attackers can use this technology to their benefit as well. "Attackers can use artificial intelligence, for example, to automate phishing emails or other attacks that until now have required significant human effort" (Kello, 2017). The U.S. will not only have to focus on

development of cyber defense but also prevent adversary uses of technology.

Social engineering and phishing attacks are still one of the most used techniques when hacking into a system. Insider threat is also a concern as current employees can cause unintentional or intentional data breaches. Cybersecurity training and awareness can be used to prevent such attacks. The U.S. needs to continue to focus on cybersecurity workforce to prevent attacks from both inside and outside the organization. Cybersecurity higher education can help influence students to join the cybersecurity field and help alleviate the cybersecurity workforces shortage.

Just as cyber threats originate from outside the U.S., defending U.S. national security from cyber threats will require cooperation with partners outside the country. Cybersecurity threats know no boundaries and will often originate from foreign nations. Collaboration with allies and raising awareness for a universal standard of cybersecurity can help the U.S. defend against cyber threats. The U.S. can use both bilateral and multilateral agreements with foreign nations to share information about cybersecurity threats.

Cybersecurity is a very broad topic that involves many aspects of technology. Cyber threats to national security are imminent and can originate from domestic or foreign sources. There are many things that can be done to prevent cyberattacks including but not limited to developing technology, influencing cybersecurity policy and education, and building a cybersecurity workforce. Collaboration with partners inside and outside the government will create a more secure cybersecurity environment and prevent cyber threats.

## 2.0 The Cyber Threat Landscape

Cybersecurity threats can emerge from nation-states, cybercrime organizations, hacktivists, terrorists, or even insiders. Nation-states like China and Russia sponsor offensive cyber operations against the United States for the purposes of espionage, intellectual property theft, and disruption. Cybercrime actors are motivated primarily by financial gain and rely on ransomware, attacks, and phishing scams as sources of income. Ideologically motivated actors or hacktivists use cyber means to forward their agendas and can attack government agencies or corporations to raise awareness (Singer and Friedman, 2014). Insider threats come from current or former employees and contractors who possess systems access. Today's threat environment is constantly evolving due to technological advancements and the convergence of critical infrastructure. As more governments, businesses, and citizens become dependent on technology, more opportunities will arise for threat actors to take advantage of.

The current threat environment is one that continues to evolve at a rapid pace. Today we live in a world of cybersecurity convergence. Nation-states are beginning to team up with cyber criminals to make attacks more resilient and harder to attribute. Independent hackers and terrorists are also using state level tooling which was made publicly available. This makes it difficult to attribute who the real actor is behind an attack. The threat environment today is one where we must focus on threats both inside and outside of our networks (Kello, 2017).

### 2.1 Nation-State Cyber Actors

Nation-state actors are sponsored or affiliated with governments and their goal is most likely advancing geopolitical, military, and economic interests. Nation-states actors are among the most skilled and well-funded threat actors targeting US interests. They tend to target US critical infrastructure owners and operators, academia, military, private sectors, political organizations, and more. Due to their level of funding and skill set, these actors typically use advanced tactics, techniques, and procedures (TTPs) that include zero-day vulnerabilities and advanced persistent threats (APTs).

The countries that have been reported to target U.S. government agencies and other organizations have been China and Russia (Rid and Buchanan, 2015). These attacks are usually well developed and covert so that attackers can go unnoticed in a system for long periods to steal as much data as possible. Nation-state actors conduct cyber espionage attacks, steal intellectual property (IP), wage influence campaigns, and could cause harm to critical infrastructure.

The main difference between nation-state actors and other cyber threat actors is the scale of their attacks and specific agenda that they follow. Nation-state attacks focus on targeting other countries to fulfill political goals. If critical infrastructure was attacked it could cause significant damage to the population. Detecting these attacks can be difficult because nation-states may attack through intermediaries.

The US currently has strategies in place to help prevent attacks from occurring from nation-states such as cyber intelligence and sharing information with cyber networks all over the world. The US has also started to include cybersecurity into the Defense Policy (Kello, 2017).

### 2.2 Cybercriminal Organizations

Cybercriminal organizations represent one of the largest actors in cyberspace due to monetary incentives being the main driving force behind their attacks. Cybercriminal groups are generally well-organized businesses that operate with a particular set of skills and can include anything from leaders and managers to software engineers and people with knowledge specific to the company they are targeting. Examples of cybercriminal activity include ransomware, identity theft, financial fraud, and selling credentials on the Dark Web. Cybercriminals have also been known to use cryptocurrencies to protect their identity when completing transactions.

We have seen several high-profile ransomware attacks in the past where malware was used to encrypt a user's data and force them to pay a sum of money to restore access to it. These attacks have targeted hospitals, cities, and governments leading to millions of

dollars in damages (Singer and Friedman, 2014). Cybercriminal groups have also used phishing emails as a way to gain initial access to a network.

The main reason cybercriminal organizations continue to pose such a threat is due to their ability to operate from any location. International crime rings have been known to consist of members from multiple countries, causing jurisdictional issues when fighting cybercrime. Also, as we have already stated cybercriminals tend to operate as businesses and will align themselves with nation-states when it benefits them.

Like with most threats in cyberspace, there are steps that can be taken to prevent attacks from cybercriminal organizations. Enabling multi-factor authentication, keeping software up to date, and training employees are great first steps to preventing a breach. As a government, it is important to have strong cybercrime laws and international partners in place to prevent these types of attacks. However, cybercriminals will always find a way which is why they will continue to pose a threat (Kello, 2017).

### 2.3 Hacktivists and Ideological Actors

Hacktivists and ideological actors attack for their own agenda or belief system and want to make a statement with their attacks rather than monetize from them. Hacktivists specifically want to get their voices heard by attacking high-profile organizations to expose information that they want the public to know about. This usually consists of website defacements, DDoS attacks, data leaks, and spam social media posts.

Attackers that fall under this category do not typically have as many resources as a state-sponsored group or organized crime group would. They can, however, cause large-scale damage if they work together. In terms of responding to attacks from hacktivists, this comes down to a lot of prevention. Looking out for strange online posts about your organization and preparing an incident response plan can go a long way. There are always new groups popping up and since a lot of hacktivists act as lone wolves, it can be difficult to know when you will become their next target (Singer and Friedman, 2014).

Attack techniques have become more sophisticated over the years as more cyber tools are found online. What used to be advanced attacks that not many people knew about are now simple steps that anyone can do online. Ideological attackers can even be used as pawns for nation-states if they want to overlap in cyber-attacks.

Ideological actors want to further their agenda and push their goals. These types of actors want to cause disruption and again, not necessarily for money. Preparation for these types of threats can be done by researching what each group's agenda is and what they are likely to target.

### 2.4 Insider Threats

Insider attacks are considered one of the hardest threats to detect because they often come from people already inside your environment, such as current or former employees or contractors who already have some sort of authorization access to the company's network and data. Insider threat could also come from business partners who have some access to your data.

Insider attacks are both unintentional and purposeful. Either way, both can cause serious damage to an organization. Some examples of insider threats are information breaches, intellectual knowledge being stolen or sold, and threats to national security.

Intentional attacks on data come from an individual who wants to exploit the organization's data for whatever reason. People who intentionally attack your data are doing so for personal gain, maybe wanting to get back at the company for firing them or other disputes.

Unintentional threat could be someone who doesn't know any better and could get tricked by a phishing email. Employees could also accidentally come across sensitive data that they are not supposed to see or access.

Insider attacks are human attacks which is why we must study human nature when it comes to cyber security (Greitzer and Frincke, 2010).

It is hard to detect insider attacks because you generally trust the people who have access inside your network. Installing firewalls and anti-virus software will not stop these types of attacks.

You can help prevent insider attacks by installing user behavior analytics software, implementing user controls and permissions, and monitoring your network 24/7.

Ensuring that your employees are trained and know what they are doing will also decrease your chances of an insider attack.

Insider attacks can be human-made or programmed to do certain activities. It is vital to have balance in cybersecurity and paying too much attention to one threat will leave your company vulnerable to another.

Employees want changes to happen right now, but in cybersecurity, it takes time to gather information and discover where the threat is coming from. Once you know what you are up against, you can create a plan to prevent that type of attack from happening again (Greitzer and Frincke, 2010).

## 3.0 Cyber Threats to Critical Infrastructure

Critical infrastructure refers to assets that are essential to U.S. national interests. Energy, utilities, transportation, healthcare, and communication systems are vital resources that drive the economy and keep the country safe. However, they have become more interconnected and digitalized over time, leading to increased cyber vulnerabilities. The frequency, scale, and sophistication of cyberattacks against critical infrastructure are increasing every

year, making it harder to defend and posing significant threats to national security.

Most modern infrastructures operate using industrial control systems (ICS) and operational technology (OT), which controls devices and equipment. Many of these systems were originally designed to operate without an internet connection. However, network connectivity was added to improve efficiency and enable remote access and monitoring. This has dramatically expanded the potential attack surface (Lim, 2026). Modern ICS/OT now face numerous threats from malicious software, ransomware, and advanced persistent threats (APT). Left unchecked, these threats could leverage vulnerabilities to cause catastrophic disruptions to critical services with severe societal impacts.

Threat actors that target critical infrastructure include nation-states, cybercriminals, and hacktivists. Nation-state actors are the biggest threat since they have the resources and motivation to carry out long-term cyberespionage campaigns. Many foreign countries have organizations that target U.S. critical infrastructure to maintain persistent access for future sabotage or intelligence gathering operations. China and Russia continue to sponsor cyberattacks against U.S. infrastructure for intelligence gain" (Lim, 2026). These attacks have leveraged novel techniques such as "living-off-the-land", where attackers utilize native tools to avoid raising suspicion. Additionally, CISA recently released an alert regarding several foreign countries that have historically targeted U.S. critical infrastructure.

Cybercriminals are another threat actor group that has caused significant concern in recent years. Unlike nation-states, cybercriminals typically act for financial gain. The healthcare sector has seen multiple ransomware attacks against hospitals attempting to extort money by encrypting critical files. Similarly, pipeline companies and municipalities have also been targeted by cybercriminals. Many critical infrastructure networks still suffer from poor cybersecurity hygiene, like weak authentication systems, outdated software, and lack of network segmentation (Lim, 2026). Successful attacks against critical infrastructure can be disastrous. As these systems are inherently public-facing, citizens' lives can be at risk when they are attacked.

Over the past few years, there has been a worrying trend of threat actors shifting focus. Organizations used to worry about cyber threats exfiltrating sensitive data. However, threat actors are increasingly seeking access to vital systems and want to remain undetected for as long as possible" (Lim, 2026). Cyber threat actors can gain persistent access to critical infrastructure systems and activate the attack when the time is right. If successful, they can cause power, water, or transportation grid to go offline during a crisis, creating national security concerns.

As more advanced technologies are adopted by critical infrastructure, attackers are finding new ways to exploit systems. Artificial intelligence (AI) technology can be used in cyber-attacks to automate vulnerability research, create phishing emails, and conduct adaptive attacks. Cyber actors are already leveraging AI to increase scale and speed attacks against critical infrastructure" (Lim, 2026). AI will only continue to grow, and attackers will most likely take advantage of it. However, cybersecurity defenders are also adopting new technologies and cannot keep up with the rapid development of new vulnerabilities.

Attackers typically take advantage of exposed services, open ports, and old software vulnerabilities to gain access to networks. Through basic cyber hygiene, many cyber-attacks against critical infrastructure could be avoided. Lim states that, "43% of initial intrusions to critical infrastructure start by exploiting preventable vulnerabilities like exposed remote desktop services, unmaintained hardware, unused cloud storage accounts, and vulnerable default passwords" (2026). As infrastructure becomes larger and more complex, maintaining systems will become more difficult.

Since many infrastructure sectors are interconnected, cyberattacks can become significantly worse if critical systems are affected. A breach in one sector can cause ripple effects across other sectors. For instance, cyberattacks against the energy sector can black out whole cities, taking down hospitals, banks, supermarkets, and more. Because of this network of dependencies, critical infrastructure presents an attractive target to cyber adversaries.

Recent examples of cyber threats to critical infrastructure include targeting an organization's actual technology to gain access and cause damage. Cyberattacks against PLCs (programmable logic controllers) have recently been on the rise. This form of operational technology allows users to automate processes. If a cyber attacker were to gain access to a PLC, they can cause downtime, destroy physical equipment, and potentially harm humans.

Although there are many ways critical infrastructure can be cyberattacked, there are also shortcomings that cause weakness. Many state, local, tribal, and territorial (SLTT) governments who operate critical infrastructure face financial restrictions and shortages of skilled cyber workforces. Legacy technologies that are difficult to upgrade or patch also pose cybersecurity weaknesses. Lastly, since critical infrastructure is run by both public and private entities, there are often poor information-sharing systems.

Securing critical infrastructure is crucial to national security and requires a whole-of-government and whole-of-society approach. Cyber threat actors are becoming more sophisticated while technology and infrastructure are constantly growing and becoming more complex. It is important that cybersecurity is developed alongside new technologies to prevent cyberattacks from penetrating critical systems.

## 4.0 Economic and National Security Impacts of Cyber Threats

Cybersecurity threats are considered one of the most challenging dangers for economic security and national safety. The US national security heavily relies on computer networks and cyber systems that are vulnerable to cyber threats, whose consequences could hurt the economy. The cyber realm may strongly impact the economy by destabilizing financial markets, shaking trust in

government institutions, disclosing confidential information, and weakening US national security. Therefore, there is a great importance to analyzing economic and national security cyber threat issues to better understand how to protect the US national security against them.

Cyber threats against businesses and governments lead to direct and indirect economic consequences that impose additional costs to organizations. Direct economic cyber threat implications include expenses that a company should cover to restore its regular operations after an attack. For instance, cybercrime damage costs worldwide are going to cost trillions of dollars per year by 2025, and the US economy will also share a huge loss (Smith, 2022). When ransomware penetrates private corporations or governmental institutions' systems, it may lock the whole system for days or weeks until the company pays the ransom. Thus, apart from the amount of money that should be spent on restoring the company from cyber threats, there is a loss of revenue during that period. Other direct cyber threat consequences that businesses may face are liability claims, regulation fines, and reputational damage.

Indirect cybercrime consequences that influence economic security include supply-chain interruption. If, for example, a company provides shipment for clients' goods and services and experiences a cyber-attack, it may affect hundreds of firms that required its services. Cyber threats may also aim at stealing intellectual properties that give firms their competitive advantages and allow them to provide innovative products to customers. In this case, if foreign countries or foreign agents gain access to competitive intelligence about US companies, America will lose its place in the market (Jones and Patel, 2021).

Cyber-attacks may affect the stock market and the economic stability of businesses by targeting banks, shares, and monetary exchanges. Stock markets may panic because of cyber threats, or just the rumors of potential cyber threats can create uncertainty. Cyber threat actors can target anything related to money transfers, which can get more vulnerable when using digital channels. With the development of online banking and declining usage of cash, cyber attackers have more opportunities to target US economy's weaknesses.

Cyber threats against the nation's security may have disastrous consequences as well. First of all, critical infrastructure is under danger from cyber-attacks. Cyber criminals may target electricity grids, water systems, airports, and railway systems, and data facilities. If such utilities are disrupted, people may be in danger of death. For example, if attackers bring down electricity, it will mess up the emergency alarms, air conditioning, heating, and other life-supporting systems. Healthcare will decline as well, which will also result in death. Such dangers are posing threat to national security as it cannot protect its people if critical infrastructure is under attack. Critical infrastructure cyber threats may cause damage to the military because the electricity and data centers power almost every military action.

Nation-state cyber threats are one of the biggest dangers to US security. Nation-states often include threat actors who try to sabotage the United States using their intelligence to guide them. Nation-state cyber espionage is a significant threat to national security as it may leak important information about US defense. If attackers gain access to important documents about the US's future plans, allies, and actions, they may use them against America.

Cyber-attacks can also be used as a weapon against the US. Countries may organize cyber-attacks that can cause significant damage to weaken America's power. The issue with cyber-attacks is that attackers are hard to trace, meaning they can get away with such crime. Other countries can benefit from cyber-attacks to increase the chances of their victory while decreasing America's.

Information warfare is also a great threat to national security. Foreign entities can spread disinformation about the government and important states people. Spreading false information may decrease public approval and cause conflicts. As politics is split into parties, cyber-attacks may increase tension between democrats and republicans which may pose a threat to the nation's security. Civilians play a great role in the nation's security as they have to protect their country if the need arises.

Military can also be a target of cyber-attacks which can negatively affect national security. The army uses computers to operate drones, encrypt their communication, and do calculations. If attackers hack the military's system, they can cause soldiers to attack allies, provide the enemy with our secret information, and much more. Airplanes, missiles, and other vehicles use computers to fly and shoot. If there is someone on the other side who can control those machines, it would be a disaster for US national security.

National security and economic security are tightly connected. If one of them suffers from cyber threats, it can dramatically decrease the other. If America's economy is under attack, it will decrease America's power. If America's national security is under attack, it can make citizens less confident about their economy.

Cybersecurity threats may have severe consequences on America's economy and security. As was mentioned before, cyberattacks can target anything based on computers and the internet. The problem with cyber threats is that it grows every day, and new viruses are being created every day. There are three categories that cyber threats may pose to America: direct, indirect, and cyber-attacks. Cyber-attacks can decrease employees' confidence, cause other countries to attack, cause attackers to invade and steal intellectual properties.

Cyber-attacks can greatly affect the economy and national security of America. Although America has one of the most robust cyber security systems, they can always be better. The US needs to constantly evaluate their weaknesses and allocate funds to cover them. Cybersecurity experts should collaborate to find better ways to protect America from cyber-attacks.

## 5.0 Emerging Technologies and Cybersecurity Challenges

Cybersecurity concerns are inherently tied to emerging technology. Emerging technologies globally are rapidly changing the digital world we live in, creating opportunities for positive digital transformations. However, along with these technologies come heightened cybersecurity risks that Americans will be faced with. Technologies that will shape the future cybersecurity landscape include artificial intelligence, quantum computing, internet of things, 5G, and edge computing. As these technologies develop and change the threat landscape, they will be leveraged to increase efficiencies and improve the performance of essential systems but also give attackers new ways to exploit vulnerabilities and harm organizations. For this reason, it is more important than ever for lawmakers and those in the cybersecurity field to understand how to manage cybersecurity risks within emerging technologies.

Artificial intelligence is perhaps one of the most impactful emerging technologies. This technology can be used for both cybersecurity defense and offense. Attackers are also taking advantage of AI to increase the complexity and effectiveness of their attacks. Phishing attacks can be automated, artificial intelligence can be used for social engineering with deep fakes, and malware can rewrite and create new code as it spreads. This will allow more attackers to get into the game as they will not need extensive skills or knowledge to take advantage of AI technology. National security concerns include preventing attackers from taking down essential systems and stealing intellectual property and private information from government organizations.

The internet of things is another emerging technology that poses massive cybersecurity concerns. There will be more connections than people this coming year. Cybersecurity experts and leaders need to focus on securing IoT devices because they are often insecure by design. Most IoT devices do not come with cybersecurity technology embedded, or even updates on the software. With multiple internets of things devices penetrating critical infrastructure industries like health, energy, and transportation, a cyberattack on these systems can cause severe damage and even threaten life. Some national security concerns would include damage to critical infrastructure and the threat to citizen's lives.

Quantum computing is an emerging technology that could break the encryption that we use to keep our cybersecurity systems today. If attackers can gain access to quantum computers, they can collect encrypted data to decrypt later. It is hard to predict how long it will take to build a quantum computer but know that it is decades away. The United States should be concerned about quantum computers because if adversaries get access to quantum technology, they can steal private intel on government organizations, steal money from banks, and wreak havoc on some critical security systems.

5G and edge computing are emerging technologies that will work hand in hand. The insecure interfaces will increase the risk for organizations by facilitating data access. 5G and edge computing will cause an increase in mobility, which will lead to real-time data functioning. This will be used to allow self-driving cars, feature in smart cities, and run operations in the military. There is also concern for hardware and software being sourced from anywhere around the world, which will increase risk for companies because they do not know where their products are coming from.

All of these emerging technologies are causing the cyber-attack surface to expand at an alarming rate. As companies and organizations transform digitally by utilizing new technologies, they are increasing their attack surface. There will be many technologies to understand and keep up with. Many of these technologies will most likely be integrated into some form another. National security concerns would include the government not knowing every vulnerability of the software that they are using.

Cybersecurity professionals are already having a hard time keeping up with current attack vectors. As new technologies develop there will not be enough cybersecurity professionals that understand these newly released technologies to defend against attacks. Future cybersecurity workforces will have to know numerous technologies and how they can effectively be used in cyber-attacks. This is not just a problem that the United States will face but worldwide.

We need to start thinking about cybersecurity from a resilience standpoint. We need to start building systems and technologies with cybersecurity built into them. We also need to know how to react if we do get attacked and have a plan of action that can be executed. There should be a collaboration between organizations and the government to prevent large attacks from occurring. We could share information about attacks and where our weaknesses are.

Lastly, we need to start controlling our technology by introducing policies and regulations. We do not have regulations for numerous technologies that we use daily. New technology is being released faster than regulations can be developed and put into place. Regulations can help prevent cyberattacks and define standards that companies should follow when creating new technology.

All of these emerging technologies have the potential to change the cybersecurity landscape. There could be new technology developed that can prevent cyberattacks before they happen. But with new technology comes new attacks and vulnerabilities that we have never seen before. The United States will need to defend against threats from adversaries who are also using these new technologies to target organizations.

## 6.0 U.S. Cybersecurity Policies and Strategies

Today, cyberspace faces threats characterized by increasing sophistication, durability, reach, and complexity. Recognizing this risk, U.S. cybersecurity policies are national and multifaceted, comprising both offensive and defensive elements across various levels of operation and leadership. In particular, The White House, through its cybersecurity strategy (2023), emphasizes resilience as its primary objective, approaching cyber policy via federal leadership and coordination across national institutions; public-

private partnerships; international alliances; innovation and technology; and research development.

Arguably the largest U.S. national cyber policy development is its focus on resilient practices that aim to reduce cyber risks. Announced goals of the 2023 National Cybersecurity Strategy are to develop "a defensible, resilient digital ecosystem where cyberattacks are harder to launch and less profitable to execute." Instead of having agencies and organizations "defend everything," the new way of thinking is centered around getting ahead of threats, crippling cyber-attacks methods, and quickly recovering from attacks should they occur. Officials outline five pillars which break down this strategic approach: defending critical infrastructure, disrupting adversaries, shaping marketplace behavior, investing in the future, and partnering with allies. The policy categories that stand out as change or add to previous efforts focus on critical infrastructure and shifting responsibility to companies.

Protecting critical infrastructure has been and will continue to be a priority for the United States due to their importance to national security. However, there has been a noticeable shift to ensure that cybersecurity and risk management policies are mandatory and reinforced by standards. While the cybersecurity of critical infrastructure has typically been left up to organizations to self-regulate, the 2023 strategy shifts towards shifting responsibility to companies that own and operate software, hardware, and systems prevalent in critical infrastructure. Positioning cybersecurity as a priority to company owners and operators will help enforce the development of secure-by-design products and services.

While cybersecurity has typically been the responsibility of an organization or system's end-user, U.S. cyber policy is shifting toward holding companies more accountable for cybersecurity standards. Cybersecurity standards are often created by private companies for other companies to follow. The idea that these standards are optional and useless without endorsement from the top down is no longer viable. As most technology circulating this century was developed by a small number of large companies, U.S. cyber policy is shifting towards secure-by-design requirements.

The Cybersecurity and Infrastructure Security Agency's (CISA) Strategic Plan for 2024–2026 outlines four goals which support the National Cybersecurity Strategy and emphasize acting immediately on current threats, hardening digital infrastructure, and driving security at scale. Crucial to CISA's goals is improving visibility into threats, better coordination around vulnerability disclosures, and standardizing incident response. CISA plans to meet its goals by collaborating across varying levels of cybersecurity actors from the public and private sectors. U.S. cyber policy understands that cybersecurity cannot be shouldered by the government alone and has made interagency and international cooperation a top priority.

Sharing information with allies and partners will be critical to United States cybersecurity. As most threats to national security originate from nation-states or organized groups with national backing, cybersecurity policies understand the necessity of integrating cyber defense with national defense and collaborating with other countries to promote resilience. The Department of Defense Cyber Strategy echoes this priority by committing to leveraging advantages in the cyber domain and deepening cooperation with allies. Cyber cooperation can take on many forms, such as intelligence sharing, cyber threat analysis, joint cyber exercises, and other efforts to delegitimize cyber programs of adversaries.

The United States also improves its cyber defenses by taking offensive actions against cyber adversaries when necessary. U.S. cyber policy does not just consist of defensive strategies and cybersecurity practices. The government has a plethora of tools at its disposal to combat cyber threats including but not limited to federal law enforcement, economic sanctions, and military options. Similar to how nuclear weapons act as deterrents, the United States can leverage its cyber program to impose costs on attackers.

Investing in research and development to improve cyber defenses and staying on top of cyber security innovations is another way the U.S. plans to prevent attacks. The National Cybersecurity Strategy makes this clear by calling for technological development in the fields of artificial intelligence, quantum technologies, and software engineering. Like any other technology, cybersecurity touches the lives of everyone who uses connected electronics. The same technology that can help prevent cyberattacks can be used by someone with malicious intent, which is why it is paramount that lawmakers and leaders stay ahead of the curve.

The last critical piece of the U.S. cyber policy puzzle is people. The United States needs cybersecurity professionals to execute all cybersecurity strategies. Currently, there is a cyber workforce shortage that needs to be addressed. The policy plans to address this by developing the cyber workforce through scholarships, workforce development, and education. Cybersecurity knowledge should be widespread, and policies should focus on reaching diverse groups of people when calling for cyber professionals.

The National Cyber Incident Response Plan (NCIRP) aims to provide a national framework to guide coordinated cybersecurity responses to significant cyber incidents. As cyber threats continue to evolve in size and complexity, it is important that the U.S. has strong policies and procedures in place to mitigate threats when they occur. The NCIRP was updated to align with the new cybersecurity strategy, focusing on how the Plan will operate jointly between partners in the Federal Government, State, Local, Tribal, and Territorial (SLTT) governments, and private-sector organizations.

There are several weaknesses within the current cyber policies that the U.S. should address. As cyber policy becomes more complex and intersects with more agencies and organizations, it can become difficult to coordinate every cyber node within the United States. While many of the goals within cyber policy focus on cooperation and coordination, cyber threat actors do not ceasefire during times of disagreement among national leaders. Cyber policies should continue to evolve and should identify weaknesses within procedures to act as quickly as possible.

In trying to improve cybersecurity across the nation, care should be taken to ensure that citizens' privacy is not violated. As the United States increases its cyber capabilities and continues to improve cyber defense, cyber policies should ensure that civil liberties are not at risk.

## 7.0 Strengthening Cyber Defense

Cyber defense needs to be strengthened. Currently, there is an increasing threat to our nation's security with the expanding cyberspace. Attacks from our adversaries whether that be another country, criminal organizations, and even insiders threaten our national security every day by trying to breach government systems, critical infrastructure, and private industry networks. To be able to better secure our nation from cyberattacks we need to ensure we have robust and adaptive cyber defenses. These defenses can be achieved through technology, policy, workforce, and other strategies.

One way to better strengthen cyber defenses is through technology. Using new and innovative technology can help us detect and respond to cyber threats as they occur. Artificial intelligence (AI) and machine learning (ML) are used to detect anomalies and even predict attacks. We can use this technology to automate our response to cyber threats which help reduce the dwell time of a cyberattack (Buchanan, 2020). Zero-trust is a new security model that is starting to be implemented. This model allows no access unless granted and it is something that we should start building our networks around (Rose et al., 2020).

We also need to focus on strengthening cyber defenses around critical infrastructure. These crucial assets provide our nation with energy, healthcare, transportation, and financial services to name a few. As our world becomes more digitized, our critical infrastructure becomes more connected and vulnerable to cyberattacks. The US government has been working on identifying critical infrastructure and providing cybersecurity guidelines and standards such as the National Institute of Standards and Technology (NIST) Cybersecurity framework which focuses on five functions to prevent, detect, and respond to cyber incidents (NIST, 2018).

Information sharing with public/private partnerships is another way we can strengthen cyber defenses. Since a lot of our critical infrastructure is owned by the private sector, we will need partners to help defend against cyber threats. Information sharing helps us learn from one another when it comes to cyber threats and what we can do to prevent them. An example of an information-sharing coalition is CISA's Joint Cyber Defense Collaborative (JCDC) (CISA, 2022). The JCDC helps promote information sharing between the government and private sector to work together to protect our nation from cyber threats.

In order to have strong cyber defenses, we will need people who are knowledgeable about cybersecurity. Today we are facing a cyber skills gap in which there are not enough cybersecurity professionals to meet the demand. We can start to build the cyber workforce by teaching and training students while they are in school and even giving them certifications. The National Initiative for Cybersecurity Education (NICE) has created a taxonomy that helps standardize cyber roles (NICE, 2021). Another way to build the cyber workforce is by providing cyber training for current employees and even those who are not.

We can also strengthen our cyber defenses by looking at current policy and seeing what we can do better. The US government has started to make moves to improve our cybersecurity. For example, there have been new policies that enforce federal agencies and contractors to turn on multi-factor authentication, encrypt data, and reporting cyber incidents to the authorities. We should also ensure that all agencies follow the policies that are put in place. It is also important for us to work with other countries to prevent cyber threats, especially cybercrime. Participating in cyber diplomacy can help prevent cyberattacks against the US by other countries (Klimburg, 2017).

An often overlooked but important part of cyber defense is incident response and recovery. Cyberattacks are going to happen whether you think you're prepared or not. That is why it is important to have an incident response plan in place and update it annually. Make sure that all employees know what to do if there is a cyber incident and conduct regular tests to ensure they know what to do. Simulations and cyber exercises are good ways to see how your employees and organization respond to cyberattacks. It is also good to focus on cyber resilience which allows organizations to adapt and recover from cyber incidents (Linkov and Kott, 2019).

Supply chain software and third-party vendors can provide vulnerabilities that cyber adversaries can exploit. The software supply chain has been one of the main attack surfaces that cyber criminals have used. To better strengthen our cyber defenses, we should look at our supply chain and identify any weaknesses. Companies should assess their third-party risk and implement strict requirements when allowing third-party vendors to do business with them. The Department of Commerce released a report on software supply chain security which includes adopting a software bill of materials or SBOM (Department of Commerce, 2021).

The human factor will always be the weakest link in cybersecurity. Cyber attackers are starting to use various social engineering methods to gain access to your networks. Phishing is one of the most known social engineering attacks where a user can get tricked into giving up their password or login information. Cyber awareness training can help users learn about the various cybersecurity risks they could face while using computers. Companies should invest in training their employees and building a cybersecurity culture. This can be done by educating your employees on the latest cybersecurity risks and holding annual security awareness weeks to reinforce those best practices like setting a strong password.

We must also continue to invest in cyber research and development. As technology advances, we as a country need to stay ahead of cyber threats with the technology we have today. Quantum technology is one example of technology we should be

investing in. The more we are able to research these technologies allow us to find ways to use them but also prevent others from using them against us.

In conclusion, there are many ways we can improve our cyber defenses. Cyber defenses should include people, technology, and policies we can use today while looking toward the future of technology. As cyber threats evolve, we will need to adapt our cyber defenses to meet new threats. By building strong cyber defenses, we can help ensure our nation is protected from cyber threats.

## 8.0 Future Challenges in Cybersecurity

The current and future trends in cybersecurity provide numerous challenges that affect U.S. national security. Cybersecurity is becoming more complex every day as malicious cyber actors are constantly evolving their tradecraft. This digitalization of technology and dependency across infrastructure increases the complexity level of the cyber domain as adversaries find new vulnerabilities to exploit. In conjunction with nation-state attacks and criminals, advances in technology pose an emerging threat to U.S. cyber defense strategy. This paper discusses five of the most important challenges that cybersecurity will provide in the future and how they will impact the ability to defend U.S. national security.

As cyberattacks evolve, they will become more sophisticated. Today's cyber threats are highly complex and target multiple domains to avoid detection. For instance, APTs, zero-day vulnerabilities, polymorphic malware, fileless attacks, and others have made attacking systems easier for adversaries than ever before. These attacks can go undetected for months, allowing attackers to gain a firm grasp on corporate and defense networks. As cyber threats become more complex, they will make it more challenging to defend against attacks that target U.S. national security.

State-sponsored attacks will continue to pose a significant threat to cybersecurity. Given the global competition between world powers, it is no surprise that cyberspace has been utilized to penetrate each other's networks. Not only are nations attacking each other, but they are targeting critical infrastructure and industrial control systems (ICS). As agencies rush to secure their IT systems, adversaries are focusing on ICS and operational technology (OT) systems. Attacks on critical infrastructure will increase, which will affect U.S. national security because many essential services rely on cybersecurity.

The attack surface is expanding at a global level. With the expansion of digitalization and new technology, more vulnerability exists within the cyber domain. For example, cloud computing has made it easier than ever to store information on various networks, which could potentially be accessed by cyber actors. As more technology advances, it is growing on a scale that we are unable to secure, creating vulnerabilities that did not exist before. Cybersecurity threats will expand as the surface attack grows, which will make it more difficult to defend vital networks.

Advances in technology are one of the benefits and drawbacks to society. While new technology can enhance cybersecurity, they can also be used against us. In particular, Artificial Intelligence (AI) has been a gamechanger in many corporate environments by providing robust options to threat hunting and security analysts. As powerful AI programs continue to be introduced, it is easy to see how they can be manipulated by cybercriminals. AI is a powerful tool that could be used to scan for vulnerabilities and launch massive attacks against defensive networks. As technology continues to advance, cybersecurity will have a harder time defending against enemies that have similar technology.

One of the issues that has been a topic of discussion for years is the lack of cybersecurity professionals. The skills gap in cybersecurity has increased, which could pose a threat to national security. If there are not enough people educated or trained in cybersecurity, how will we expect to defend against cyber threats? There is a global shortage of cybersecurity skills that could potentially increase the risk of attacks if left unsolved. Educating and creating a workforce that specializes in cybersecurity is critical to defending against cyber threats.

The supply chain is a significant weakness when discussing cybersecurity. Most information systems consist of hardware, software, and services that come from multiple sources. This makes it difficult to know what you do not know, which allows cyber actors to exploit numerous systems through the supply chain. For example, software supply chain attacks can provide malicious actors with access to thousands of victims through one attack. GAO determined that cyber security of the supply chain is important and requires more attention to ensure national security systems are not compromised.

Cybersecurity incidents involving infrastructure will be one of the biggest challenges of the future. Infrastructure attacks can include anything that compromises the physical devices we use every day. As our infrastructure continues to become more digitized, they also become more vulnerable to cyber-attacks. According to the Cybersecurity and Infrastructure Security Agency (CISA), federal agencies reported over 35,000 cyber-attacks in 2020. Securing infrastructure will be a problem in the future as more devices connect to the internet.

The United States does not have an effective cybersecurity strategy. While there has been significant improvement, there are still gaps in the current program that cyber actors will take advantage of. Today we face issues with coordination, implementation, and oversight of our cybersecurity programs. As cyber threats evolve, it will be increasingly difficult to defend against enemies who can attack at will. Cyber threats will only get worse if we do not have a set plan to manage and monitor cybersecurity.

Cybersecurity is no longer just a cybersecurity issue; it's a national security issue. Today, cybercriminals can attack our economy, foreign policy, and military at any given time. With how complex cybersecurity is, it will be difficult to defend every attack that occurs. As more devices connect to the internet, our nation's

security becomes more vulnerable to cyber-attacks. Cybersecurity is something that we will continue to worry about until we can devise a method to prevent attackers from succeeding.

## 8.0 Conclusion

Cybersecurity threats are a rapidly growing danger to United States national security. Nation-state actors, cybercriminal groups, and ideological operatives have shown great interest in penetrating digital networks to steal information, damage critical infrastructure, and conduct espionage.

Digital transformation has allowed cybercriminals to broaden their attack surface and find new vulnerabilities to exploit. Additionally, advances in artificial intelligence and the internet of things have created further challenges to cybersecurity.

National security can only be protected through collaboration between federal government, private sector groups, and international partners. United States agencies and organizations should focus on implementing strong cybersecurity architecture, developing cyber workforces, and cooperating with international partners on cyber defense.

## References

[1] The Impact of Cybersecurity Breaches on Patient Data Privacy in U.S. Healthcare Systems. Available at: DOI: 10.29322/IJSRP.14.11.2024.p15511

[2] Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation at: DOI: 10.29322/IJSRP.13.12.2023.p14419

[3] Cyber Threats to National Security: An In-depth Analysis of the United States Landscape at: DOI: 10.29322/IJSRP.13.12.2023.p14415

[4] GAO (2024) High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation. Available at: https://www.gao.gov/products/gao-24-107231

[5] GAO (2023) Cybersecurity Strategy and Oversight Challenges. Available at: https://www.gao.gov/products/gao-23-106415

[6] National Academies (2025) Cyber Hard Problems: Focused Steps Toward a Resilient Digital Future. Available at: https://www.nationalacademies.org

[7] World Economic Forum (2026) Global Cybersecurity Outlook 2026. Available at: https://www.weforum.org

[8] ScienceDirect (2023) Cyber Security: State of the Art, Challenges and Future Directions. Available at: https://www.sciencedirect.com

[9] TechRadar (2026) Why Modern Cyber Conflict is a Global Skills Challenge. Available at: https://www.techradar.com

[10] The Verge (2026) Anthropic AI Model and Cybersecurity Risks. Available at: https://www.theverge.com

[11] Buchanan, B. (2020) The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press.

[12] CISA (2022) Joint Cyber Defense Collaborative. Available at: https://www.cisa.gov (Accessed: 12 April 2026).

[13] Department of Commerce (2021) The Minimum Elements for a Software Bill of Materials (SBOM). Washington, DC: U.S. Government.

[14] Klimburg, A. (2017) The Darkening Web: The War for Cyberspace. New York: Penguin Press.

[15] Linkov, I. and Kott, A. (2019) 'Fundamental concepts of cyber resilience: Introduction and overview', IEEE Systems Journal, 13(4), pp. 3716–3717.

[16] NICE (2021) National Initiative for Cybersecurity Education Strategic Plan. Available at: https://www.nist.gov/nice (Accessed: 12 April 2026).

[17] NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD: National Institute of Standards and Technology.

[18] Jones, M. and Patel, R. (2021) Cybersecurity and Economic Growth in the Digital Age. New York: Routledge.

[19] Lewis, J.A. (2020) Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies.

[20] Rid, T. (2019) Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux.

[21] Smith, A. (2022) 'The global cost of cybercrime', Journal of Cybersecurity, 8(2), pp. 115–130.

[22] Taddeo, M. (2020) 'The ethical challenges of cyber operations in national security', Philosophy & Technology, 33(2), pp. 187–205.

[23] Greitzer, F.L. and Frincke, D.A. (2010) 'Combining traditional cyber security audit data with psychosocial data', Insider Threats in Cyber Security, pp. 85–113.

[24] Kello, L. (2017) The Virtual Weapon and International Order. New Haven: Yale University Press.

[25] Rid, T. and Buchanan, B. (2015) 'Attributing cyber attacks', Journal of Strategic Studies, 38(1-2), pp. 4–37.

[26] Singer, P.W. and Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press.

## Authors

**First Author** – Surya Prakash Reddy Pakanati.
**Second Author** – Olafuyi Olajide.
**Third Author** – Olafuyi Basiru, bolafuyi01@gmail.com.