Cybersecurity Strategy, Law, and Policy Group Assignment 

CMIT 495: Current Trends and Projects in Computer Networks and Security

Gene Anderson

By:

Group 7

Kristina Keefe

Luis Tinajero

Tri Ho

Contents

[Introduction (Tri Ho) 3](#_Toc160391447)

[Part 1: National Security Strategy and Cybersecurity (Tri Ho) 5](#_Toc160391448)

[Part 2: Public/Private Partnerships (Tri Ho) 9](#_Toc160391449)

[Part 3: Private Sector Organizations (Luis Tinajero) 14](#_Toc160391450)

[Part 4: Protecting Critical Infrastructure and the Homeland (Luis Tinajero) 16](#_Toc160391451)

[Part 5: Cybersecurity Technologies (Luis Tinajero) 19](#_Toc160391452)

[Part 6: Ethics in Cybersecurity (Kristina Keefe) 21](#_Toc160391453)

[Conclusion (Kristina Keefe) 25](#_Toc160391454)

[References 29](#_Toc160391455)

# Introduction (Tri Ho)

This white paper describes the current governance, policy, and legality of cybersecurity and data privacy in the US. Comparing the US legal framework and other popular regulations, such as the General Data Protection Regulation (GDPR), gives a brief insight into whether or not a more stringent data protection regulation should be applied. This paper goes on to address the strategic importance of the public-private partnership. The Cybersecurity Act 2015 is used as a pivot document to explore further the benefits and adverse implications of the information-sharing strategy. In addition to the regulatory discussion, this paper also identifies and explores the potential application of emerging technologies such as AI, Machine Learning, and Blockchain in the context of cyber offensive and defensive capabilities. Following the discussion of technology application is the ethical use of technology in threat identification, such as the mass surveillance system in conjunction with technology. The paper is then complete with a section of actionable recommendation strategies for cybersecurity for the upcoming year.

# Part 1: National Security Strategy and Cybersecurity (Tri Ho)

* After reading the [National Security Strategy (2017)](https://leocontent.umgc.edu/content/dam/permalink/7797e833-040a-4563-9e8e-da4ce4b27a09.html), comment on the following.
  + *Should the United States create a separate cybersecurity strategy to be published alongside the National Security Strategy (NSS), or do you feel the NSS is sufficient? Why or why not?*

The National Security Strategy (2017) covers many areas of interest, from geopolitics to economy and military defense. This document sets forth four fundamental principles for the US to maintain its global dominance in all aspects of the modern world.

* + 1. Protect the American People, The Homeland, and the American Way of Life
    2. Promote American Prosperity
    3. Preserve Peace through Strength
    4. Advance American Influence

Within the cyber domain, the document also layout five priority actions:

1. **Identify and prioritize risk**; assess risk in six key areas: national security, energy and power, banking and finance, health and safety, communications, and transportation.
2. **Build defensible government networks**; use the latest technology and best practices to guarantee the optimal uptime of networking in all conditions.
3. **Deter and disrupt malicious cyber actors;** ensure correct role and privilege assigned to critical personnel, work with allies, and deliver consequences to threat actors both domestic and ashore.
4. **Improve information sharing and sensing;** improve both speed and accuracy of sharing and sensing critical information to allies and partners; invest in new capabilities to conduct cyber attacks.
5. **Deploy layered defense;** defense in depth by employing assistance from private entities to stop attack in transit before they can infiltrate the target.

The NSS provides adequate depth in many areas and serves as the framework for designing national security from 2017 forward. That said, the 2017 NSS did not address the cybersecurity piece to its proper length.

NSS 2017 was written with four main objectives, forming the four discussion pillars for the entire paper. To achieve this intended end stage, information security must be accomplished first. The information domain uniquely dissects all other domains in a comprehensive national strategy. From a typical marketing campaign to a high-stakes diplomacy policy, no single strategy can be appropriately formed and executed without good information and data. The US must maintain its superior position in information security and warfare. With it, the other four can be accomplished. Without it, the entire strategy will falter. Information security is such a big topic that it may or may not be suitable to be included in a condensed strategic document such as NSS; a separate document dedicated strictly to cybersecurity is therefore needed.

* *Consider your answer in the context of the original*[*National Strategy to Secure Cyberspace (2003)*](https://leocontent.umgc.edu/content/dam/permalink/309f36dc-ce7c-4cbe-9d55-41bc563108cc.html)*. What is not adequately addressed in the National Security Strategy (2017) as it relates to cybersecurity?*

For all intents and purposes, the National Strategy to Secure Cyberspace or NSSC 2003 covers the cyber landscape in much greater depth and breadth than the later publication. It is somewhat expected from NSSC to be an exclusive standpoint of cybersecurity versus a holistic national security philosophy. One of the prime examples of the comprehensive nature of NSSC is that it targets 12 sectors that, when combined, form the critical infrastructure of the United States versus six key domains in NSS 2017. In addition, the NSSC highlights the roles of government organizations and private institutions in a combined effort.

* The 2017 NSS did a great job defining the desirable end stage of the cybersecurity structure. The National Strategy to Secure Cyberspace NSSC (2003) was the first to acknowledge the progressive and ever-evolving nature of the cyber threat landscape. NSSC further addresses the need for adaptability and adjustment in the cyber defense framework. This aspect was left out in the NSS 2017.
* The 2017 NSS "Keep the American Safe in the Cyber Era" did well in setting the end stage for cybersecurity strategy. While it adequately addresses the importance of putting the right person on the job through privilege and role assignment, it skips the information security aspect entirely. One way to achieve information security is through proper classification/declassification protocol. This topic may sound redundant, but the number of classified information mishandling by US officials must not be overlooked as Hulse (2023) recalled the incident in Mar-a-Lago not too long ago. The NSS did not address the importance of increasing user awareness of cybersecurity. In other words, the 2017 NSS did not acknowledge and provide a framework to manage user error or human vulnerability in cyberspace.
* NSS 2017 also did not address the technical worker training and certification issue. While both documents acknowledge the need for collaboration between government entities, the private sector, and NGOs, only the NSSC 2003 provides the guiding principles for establishing a well-trained technical workforce and standardization in certification.
* NSSC also introduces and discusses the information-sharing requirements between agencies and sectors when encountering cyber threats. Information sharing lies at the heart of cybersecurity strategy on a national level. NSSC recognizes the lack of reachability of government agencies and the technological prowess of the private sector. Additionally, NSSC mentions a key characteristic of cyberspace: the majority of the internet is privately owned. Therefore, a successful national security strategy must involve private institutions such as service providers to achieve both the protection of national interest and the protection of privacy. The NSS in 2017, even though it covered privacy matters in the grand picture of national security. It did not bring up privacy matters in cyberspace.

# Part 2: Public/Private Partnerships (Tri Ho)

* After reading the [Cybersecurity Act of 2015](https://leocontent.umgc.edu/content/dam/permalink/f6be7d73-16df-4205-9dd9-b38d511c34e7.html), addresses the private/public partnership with the DHS National Cybersecurity and Communications Integration Center (NCCIC), arguably the most important aspect of the act. The Cybersecurity Act of 2015 allows for private and public sharing of cybersecurity threat information.
  + *What should the DHS NCCIC (public) share with private sector organizations? What type of threat information would enable private organizations to better secure their networks?*

In the spirit of the Cybersecurity Act 2015, DHS NCCIC should share information about cyber threats, defensive measures, recovery technique user awareness to current and upcoming threats. A prime example is the Internet Crime Compliant Center (IC3). This organization aggregates the submitted data from private sector, produces an annual report on the trends impacting the public, and routinely provides intelligence reports (IC3, 2022). Since DHS NCCIC has many established partnerships with multiple private entities, the information shared with DHS NCCIC should come in denser and richer than that of any single private organization. For example, if two private organizations do not have a pre-existing partnership, they are not obligated to inform others of any threat or mitigation strategies. With DHS NCCIC standing at the center stage, all information and defensive measures can be submitted to one body, and other private entities can significantly benefit from the latest information and better protect their system. A prime example in InfraGard, an collaborative initiative between FBI and DHS, that has over 80k membe across 50 states and terriories. InfraGard support its member by providing updated threat advisories, alerts, intelligence butletins, analytical reports, vunerabilities assessment and many other type of courses and workshops via the National Infrastructure Resilience and Security U (NISRU), according to InfraGard (2022).

* + *On the flip side, what should private organizations share with the NCCIC? As it is written, private organization sharing is completely voluntary. Should this be mandatory? If so, what are the implications to the customers' private data?*

Government agencies and the public sector share two common characteristics when it comes to cyberspace:

* + 1. Their IT architecture runs on the back of privately developed technology. For example, Microsoft developed Windows, which runs on government computers that transmit data packets through Cisco networking devices.
    2. Government worker also brings their device to work, such as smartwatches, smartphones, headphones…. Therefore, they are also exposed to everyday cyber risks and vulnerabilities like the general public.

For this reason, any identified vulnerability, patch, or update of software and hardware that is used to run, transmit, and store data should be shared with NCCIC as timely as possible, regardless of whether said piece of technology and equipment is being used within a government facility or not.

Sharing information with NCCIC should remain voluntary in good spirit, with an obligation to report cyberattacks or breaches of confidentiality that originate or discovered from private-sector infrastructure. This type of incident report can help governments agencies such as IC3 and InfraGard to formulate a report, conduct investigation, send out warning messages for others, and in some cases leading to a successful recovery of loss assets (IC3, 2022).

A group of banners with text

Description automatically generated with medium confidenceA graph of a graph of a graph

Description automatically generated with medium confidenceFigure 1: Illustration of IC3 core function that ultilize private sector incident reporting (IC3, 2022)

Figure 2: A diagram illustrating the success rate of IC3 Recovery Asset Team (RAT), courtesy of IC3.org

As it is written, personal identifiers should be omitted or removed before submission to protect the user's privacy as well. The 2015 Act requires the private entities who partner with NCCIC not to disclose any network traffic transmitting to and from the agency unless it is directly related to the risk or a case. Should this be mandatory, any noncompliance action is, in all technicalities, punitive. The sharing of information on threat indicators as a part of the cyber defense strategy is similar to casting the widest net and hoping to capture the intended target. This approach will almost guarantee irrelevant information gets mixed in with relevant information, which in turn violates the condition of the act itself for disclosure of traffic that is not directly related to cyber risk. Moreover, the sheer amount of network traffic that goes through the Internet Service Provider's network on any given day makes this task unfeasible to be mandated. A private company such as the Internet Service Provider (ISP) will either have to stay in the partnership and face the risk of being sued or opt-out and get left in the dark about upcoming cyber threats.

On the other hand, NCCIC organizations in itself is not without flaw and still susceptible to cyber attack. A case of mandated submitting of information that eventually got leak and exploited by hacker could potential damage not only the agencies reputation but also incur in asset loss for the multiple private entities. Unfortunately, such an incident actually took place in 2022 . A hacker who reportedly posed as the CEO of a financial institution claims to have obtained access to the more than 80,000-member database of InfraGard (Bajak, 2022).

* + *The government is not allowed to collect data on citizens. How should the act be updated to make it better and more value-added for the public-private partnership in regards to cybersecurity?*

The most significant debate regarding regulating virtual domains, perhaps, is the topic of privacy and anonymity. Too much anonymity and cyberspace can easily become the fostering ground for criminals and threat actors. Fortunately, the 2015 Act can remain relevant and effective by employing tag traffic and metadata. In short, metadata is the data that gives information about the format and content without disclosure of the actual data itself. Then, tag traffic ultility can be used to add more information to the type, and intended destination of data in human readable format. Tag traffic has been used quite popularly since the invention of virtual networks. When using metadata and tag traffic in conjunction, the shared information between public and private entities can remain non-specific but with higher investigational value.

# Part 3: Private Sector Organizations (Luis Tinajero)

* Review the [General Data Protection Regulation (GDPR)](https://www.gdpreu.org/) of the European Commission (EU). It includes many provisions and arguably strengthens data protection for individuals within the EU. It even includes the right to be forgotten. The United States does not have a similar regulation. There have only been a few regulations implemented related to US citizens' private data, which include medical and financial industries. Some argue implementing regulation such as GDPR in the United States would hinder innovation. They contend that the End User License Agreements (EULA) provide sufficient protections and allow the citizens to make the choice of what is and is not shared.
  + *As a private sector organization, do you believe that an equivalent to GDPR should be implemented in the United States?*

As a private sector organization, there is a compelling argument for the implementation of an equivalent to the General Data Protection Regulation (GDPR) in the United States. GDPR has set a high standard for data protection and privacy rights, which aligns with the growing concerns regarding personal data security in an increasingly digital world (European Union, 2016). Implementing GDPR-like regulations in the US could provide a more consistent and robust framework for safeguarding individuals' privacy and enhancing trust in the digital economy.

Moreover, GDPR compliance could streamline operations for multinational companies operating both within the EU and the US, minimizing regulatory complexity and legal risks associated with data handling practices. By adopting GDPR principles, organizations may also benefit from improved data governance, risk management, and customer trust, ultimately enhancing their competitive position in the global marketplace.

However, it is essential to consider potential challenges and implications for innovation and business practices. Some argue that stringent data protection regulations could impose undue burdens on businesses, particularly small and medium-sized enterprises (SMEs), stifling innovation and economic growth (Mayer-Schönberger & Cukier, 2013). Therefore, any US implementation of GDPR-like regulations should carefully balance the need for robust data protection with fostering innovation and economic competitiveness.

In summary, while there are valid concerns and complexities associated with implementing GDPR-like regulations in the United States, private sector organizations should recognize the importance of data privacy and consider the potential benefits of adopting similar frameworks to enhance consumer trust, mitigate risks, and promote responsible data practices. (GPDR, 2023).

# Part 4: Protecting Critical Infrastructure and the Homeland (Luis Tinajero)

* The [Department of Defense (DoD) Cyber Strategy 2018](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) discusses the protection of critical infrastructure and the homeland. *What does that mean to private organizations such as yours? If most critical infrastructure in the United States is owned by the private sector, what responsibility does the DoD have in this regard? Some would argue US laws are outdated and thus the DoD has little authority to assist. Others would argue US laws were purposely established such that the private sector would defend itself and not need assistance from the military. Obviously, for the DoD to assist, it would need the private organizations' data. Said another way, the DoD would need your data as a private citizen/customer of that organization. Those that believe our laws need to be updated argue giving up privacy for protection is legitimate. Others will argue that we should not give private information of citizens to the government for any reason.*
  + *As a citizen, would you feel comfortable with this? As a private organization, would you feel comfortable giving information that may contain your customers' private data to the DoD?*

As a citizen, concerns may arise regarding the privacy implications of sharing personal data with the Department of Defense (DoD). The prospect of the DoD accessing private information, including that of customers, raises valid apprehensions about potential government overreach and the protection of civil liberties. This concern is rooted in longstanding debates over the balance between national security imperatives and individual privacy rights (Solove, 2007). The principle of privacy is enshrined in various legal frameworks, such as the Fourth Amendment to the United States Constitution, which protects against unreasonable searches and seizures by the government (Electronic Frontier Foundation, n.d.). Therefore, citizens may express discomfort with the idea of private data being shared with the DoD, as it raises questions about the extent of government surveillance and the erosion of privacy rights.

  Similarly, as a private organization, there are significant considerations regarding the comfort level in providing information containing customers' private data to the DoD. Organizations are entrusted with safeguarding sensitive customer information and maintaining the trust and confidence of their clientele (Cavoukian & Castro, 2010). However, the potential collaboration with government entities, including the DoD, in cybersecurity efforts may necessitate sharing certain data for threat intelligence and incident response purposes (Schneier, 2015). Balancing the imperative to protect critical infrastructure with the duty to uphold customer privacy poses a complex challenge for private organizations

* + *Is there a third solution (middle ground) you would propose that enables privacy but also enables cybersecurity?*

A potential middle ground solution that balances privacy and cybersecurity concerns involves establishing robust data protection frameworks and fostering collaboration between the private sector and government agencies without compromising individual privacy rights. This approach aligns with the concept of Privacy by Design, which advocates for embedding privacy protections into the design and operation of systems and processes (Cavoukian & Castro, 2010). By implementing stringent data encryption and anonymization measures, organizations can mitigate the risk of unauthorized access to sensitive information while enabling secure data sharing with government partners (Kuner, 2018).

Furthermore, the development of public-private partnerships focused on cybersecurity initiatives could facilitate information sharing and collaborative defense efforts while ensuring accountability and adherence to privacy regulations (Department of Homeland Security, 2020). These partnerships may involve the establishment of Information Sharing and Analysis Centers (ISACs) or sector-specific alliances aimed at enhancing cyber resilience across critical infrastructure sectors (Council on Foreign Relations, 2018). Through these collaborative endeavors, private organizations can contribute valuable insights and resources to national cybersecurity efforts while preserving customer privacy and trust.

Addressing cybersecurity challenges while upholding individual privacy rights requires a balanced and collaborative approach between the private sector and government entities. By implementing robust data protection measures and fostering transparent partnerships, a middle ground solution can be achieved that enables effective cybersecurity without compromising privacy.

# Part 5: Cybersecurity Technologies (Luis Tinajero)

* The authors of the [National Security Strategy (NSS)](https://leocontent.umgc.edu/content/dam/course-content/tus/cmit/cmit-495/document/NationalSecurityStrategy-2017.pdf) are looking to address particular technologies that have the opportunity to revolutionize cybersecurity. They believe that blockchain technology is a revolutionary technology that has the ability to significantly improve cybersecurity.
  + *What would be your recommendation for how the NSS should incorporate this technology to the public?*

 To incorporate blockchain technology into the National Security Strategy (NSS) effectively, it is essential to prioritize education and awareness campaigns aimed at the public. This involves disseminating accessible and informative materials that explain blockchain technology in layman's terms, highlighting its potential to enhance cybersecurity and protect critical infrastructure. Additionally, the NSS should emphasize the importance of collaboration between government agencies, private sector stakeholders, and academic institutions to drive research, development, and adoption of blockchain-based cybersecurity solutions (World Economic Forum, 2018). Public-private partnerships can facilitate the integration of blockchain technology into existing cybersecurity frameworks and promote innovation in this domain. Furthermore, the NSS should advocate for the establishment of regulatory frameworks that support the responsible deployment of blockchain technology while safeguarding privacy and security concerns.

* + *Propose exactly what you believe should be written in the NSS. Specifically, explain the blockchain technology in layman's terms to nontechnical people that may be reading the NSS, give examples of how it could be used to provide revolutionary cybersecurity, include examples of how it is being used to provide cybersecurity solutions, and discuss what, if any policies* or laws should be established to mandate its use in specific industries.

**Understanding Blockchain Technology:**

Blockchain technology, a decentralized ledger system, offers secure and transparent transactions by recording data across a network. Its immutable nature ensures tamper-proof records, enhancing data integrity and trust.

**Revolutionizing Cybersecurity:**

Blockchain's decentralized structure mitigates single points of failure, enhancing resilience against cyberattacks. It offers secure authentication and encryption mechanisms, safeguarding digital assets and critical infrastructure.

**Examples of Blockchain in Cybersecurity:**

Blockchain-based identity management systems and electronic health records ensure data privacy and integrity. In supply chain management, blockchain tracks product provenance, combating counterfeiting.

**Policy Recommendations:**

* + Develop regulatory frameworks supporting responsible blockchain deployment.
  + Foster public-private partnerships for innovation in blockchain cybersecurity.
  + Invest in research to advance blockchain technology for national security.
  + Provide workforce training for effective blockchain utilization in cybersecurity.

 By embracing blockchain, the NSS strengthens national security and protects digital infrastructure (Tapscott, D., & Tapscott, A., 2016).

# Part 6: Ethics in Cybersecurity (Kristina Keefe)

* Ethical issues are at the core of what we do as cybersecurity professionals. Think of the example of a cyber defender working in a hospital. They are charged with securing the network, medical devices, and protecting sensitive personal health information from unauthorized disclosure. They are not only protecting patient privacy but their health and perhaps even their lives. Confidentiality, Integrity, Availability - the C-I-A triad - and many other cybersecurity practices are increasingly at play in protecting citizens in all walks of life and in all sectors. Thus, acting in an ethical manner, is one of the hallmarks of a cybersecurity professional.
  + *What are the ethically significant harms that may result from mass surveillance (including by government and corporations)?*

"No system of mass surveillance has existed in any society that we know of to this point that has not been abused." Edward Snowden's quote captures the reality of the dangers of mass surveillance. It can be implemented for positives like national security or simplifying logging into online bank accounts/hospital websites, but in today's world, mass surveillance can be abused and can be a vulnerability. Mass surveillance, whether carried out by governments or corporations, has become increasingly prevalent in day-to-day life, and the digital era. While some argue for its necessity in maintaining security, this practice raises significant ethical concerns. The widespread gathering of personal data without individuals' consent violates fundamental rights to privacy. Recognizing and addressing these ethical dilemmas is essential for striking a balance between security needs and individual freedoms in today's interconnected world.

Government mass surveillance has caused significant ethical concerns, such as privacy breaches and a decline in trust in institutions. Mass surveillance leads to various ethical harms, including violations of individual rights and freedoms, thus fueling skepticism toward authorities among the public. On the other hand, corporate mass surveillance has led to notable issues like data breaches, and exploitation of customers. Companies collecting extensive personal information often fail to adequately protect it, leading to breaches that expose individuals to identity theft and financial fraud. Also, when companies profit from selling personal data, it raises ethical questions about whether it's right to treat people as objects to make money from. In both sectors, mass surveillance undermines privacy, and confidence, emphasizing the urgent need for ethical considerations and regulatory oversight to address these concerns.

A graph of data breaches

Description automatically generated

Figure 3: Infographic of Large-Scale Data Breaches Affect Millions of Users. (Statista, n.d.)

In the chart above, Statista shows millions of users affected by large-scale data breaches. Because mass surveillance collects vast amounts of personal data there is a risk of date breaches making individuals more susceptible to identity theft. This data becomes attractive to cyber attackers, creating more vulnerabilities in our digital systems. Also, it can lead to complacency towards cybersecurity measures and the potential misuse of surveillance tools for harmful purposes, eroding trust in digital platforms.

* + *What are the ethically significant harms that may result from emerging technologies such as blockchain technology, artificial intelligence, and machine learning.*

As society eagerly adopts new emerging technologies ethical questions are taking center stage. While these innovations hold great promise for improving our lives and industries, they also bring ethical challenges that need careful attention.

Block chain technology can cause ethical harms of attracting criminal market, cryptojacking, owning illegal data though data trails. The main harm to cyber security could be crypto mining, making attacks on high performance computers more often like the attack on the company, Radiflow monitor water supply. (Newman, 2018) Also the inhouse ability to install software to mine cryptocurriencies on restricted areas (Russian Nuclear warhead) pose immense security theats. (BBC, 2018).

A table of text with words

Description automatically generated with medium confidenceArtificial Intelligence and machine learning have numerous ethical harms and considerations that must be addressed. The main ethical harms include data security, privacy, accountability, standards, social, accessibility, democracy, civil rights, faulty algorithmns, and bias. For example, there was an AI-assisted cyber-attack at TaskRabbit where 3.75 million customers had financial and personal data stolen, AI-enabled botnet was used to execute DDoS attack on servers. Analysts believe that an AI-enabled botnet was used. The botnet slave machines were used to execute a DDoS attack on TaskRabbit’s servers. By prioritizing transparency, accountability, and fairness the use of AI can improve cybersecurity while also protecting the rights of individuals. Below is a table of ethical concerns of artificial intelligence and machine learning in an organized proposed categorization of ethical issues. It shows the discussion of what should be addressed.

Figure 4: Overview of ethical complications with AI technology (Huang et al., 2023)

With the emerging technologies such as blockchain, artificial intelligence, and machine learning it is important to be aware of the ethical harms that could happen with incorporating them into our everyday lives. Even with the complexities and challenges these technologies can play an important role in our future society if there is discipline in ethics happens in a joint effort with scientists, engineers, users, and government policymakers.

# Conclusion (Kristina Keefe)

This white paper has provided specific recommendations on the next cybersecurity strategy, private/public partnerships, and comments on how specific technologies should be incorporated into the assessment.

* The United States should create a separate cybersecurity strategy to be published alongside the National Security Strategy (NSS). The second separate document should be dedicated strictly to cybersecurity, defining the national cyber defense posture and strategy.
* The DHS NCCIC should share any latest guidance on cybersecurity plans, assessments, and reports of cybersecurity threats along with implementation to mitigate the threat with private sector organizations.
* Sharing information with NCCIC should remain voluntary, with an obligation to report cyberattacks of confidentiality that originate from private-sector infrastructure such as data centers.
* The 2015 Act act should be updated with using metadata and tag traffic in conjunction, the shared information between public and private entities can remain non-specific but with higher investigational value.
* Private sector organizations should recognize the importance of data privacy and consider the potential benefits of adopting similar frameworks to enhance consumer trust, mitigate risks, and promote responsible data practices.
* Private organizations need to implement robust data protection measures and foster transparent partnerships, so that a middle ground solution can be achieved that enables effective cybersecurity without compromising privacy.
* To incorporate blockchain technology into the National Security Strategy (NSS) effectively, it is essential to prioritize education and awareness campaigns aimed at the public.
* NSS should advocate for the establishment of regulatory frameworks that support the responsible deployment of blockchain technology while safeguarding privacy and security concerns.
* NSS should include layman terms, examples, and solutions like blockchain’s ability to secure authentication and encryption mechanisms, safeguarding digital assets and critical infrastructure.
* Emerging technologies such as blockchain technology, artificial intelligence, and machine can play an important role in our future society if the discipline in ethics happens in a joint effort with scientists, engineers, users, and government policymakers.
* Blockchain technology is the key to unlocking the new cybersecruity era. One key advantage of blockchain is tampered-proof. One an entry is made to the log then it cannot be changed.  At the time of a new log entry, two copies will be generated: one to system log and another to a separate location that only the IT admin knows. Since every entry is made permanent as it adds to the chain, no single hacker can have enough computing power and speed to replicate the log with their fabricated version, like in APT 34.
* Blockchain capability can be greater enhanced with biometric and double encryption to generate a third key: call the section key. The section key will have the authenticated biometric and unique encryption factor with a sequence number made up from two parts: X-Y.
* Cyber security professionals should leverage AI/ML for threat detection because it has the ability to analyze data and identify anomalies in a timely matter that would be impossible for humans.
* Implementing a Zero-Trust policy will strengthen security posture by requiring verification of all entities before access is granted, minimizing lateral movement and insider threats.
* It’s important to implement a virtual cloud infrastructure with a thought out strategy including choosing reliable cloud provider, understanding responsibilities, using strong authentication and encryption, and implementing access control.
* Quantum computing will be a threat to encryption, staying up to date with post-quantum cryptography algorithms like cyrstals, falcon, and sphincs is vital to maintaining a good secure posture.

“We're still in the honeymoon phase of connectivity. Governments and corporations are punch-drunk on our data, and the rush to connect everything is driven by an even greater desire for power and market share.” Bruce Schneier explains that this age of connectivity presents complex challenges that have the possibility of unimaginable problems. With the ever-evolving technology, cybersecurity must stay up to date with current trends and be proactive for future changes. The bad actors will exhaust efforts to stay ahead of cyber defenders, that is why it is important to stay vigilant and educated. Its vital to embrace new technology as it can streamline processes and strengthen security for systems. By implimenting new technologies smoothly with the correct policies and mindset of making sure its thouroughly assessed of ethics, proof of concept, and vulnerabilities, private-sector and government entities can work together to mitigate the attack vector in significant industries like infrastructure, healthcare, energy, and finance. To conclude, Bradley B Dalina explains the crucial necessity of cybersecurity, “In this fast-growing digital era, cybersecurity awareness must be introduced as part of the new social norms for the basic units of society, for it is no longer an option but a crucial necessity.”

# References

Bajak, F. (2022, December 15). Hacker claims breach of FBI’s critical-infrastructure portal | AP News. *AP News*. Retrieved March 3, 2024, from <https://apnews.com/article/technology-business-hacking-government-and-politics-4f2eeabfd6f3a998a374c1bca5c1fbc6>

BBC.(2018). Russian nuclear scientists arrested for ‘Bitcoin mining plot’. Retrieved from [www.bbc.com/news/world-europe-43003740](http://www.bbc.com/news/world-europe-43003740)

C. Huang, Z. Zhang, B. Mao and X. Yao, "An Overview of Artificial Intelligence Ethics," in IEEE Transactions on Artificial Intelligence, vol. 4, no. 4, pp. 799-819, Aug. 2023

Cavoukian, A., & Castro, D. (2010). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.

Council on Foreign Relations. (2018). Cybersecurity and Infrastructure Security Agency (CISA). Retrieved from <https://www.cfr.org/backgrounder/cybersecurity-and-infrastructure-security-agency-cisa>

Department of Homeland Security. (2020). Critical Infrastructure Security. Retrieved from <https://www.dhs.gov/cisa/critical-infrastructure-security>

Electronic Frontier Foundation. (n.d.). Surveillance Self-Defense. Retrieved from <https://ssd.eff.org/en/module/legal-protections-us-citizens>

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.

GDPR: General Data Protection Regulation. GDPR EU. (2023, June 15). <https://www.gdpreu.org/>

Goodreads : Cybersecurity Quotes: Goodreads (2024) <https://www.goodreads.com/quotes/tag/cybersecurity>

Hulse, C. (2023, January 27). Mishandling of classified information has Congress asking questions. *The New York Times*. Retrieved March 3, 2024, from <https://www.nytimes.com/2023/01/27/us/politics/classified-info-congress-pence-trump-biden.html>

InfraGard. (2022, February 24). *InfraGard Redesign 2022* [Press release]. Retrieved March 3, 2024, from <https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf>

IC3. (2022). 2022 Internet Crime Report. In *IC3*. Federal Bureau of Investigation. Retrieved March 2, 2024, from <https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf>

Infographic: Large-Scale Data Breaches Affect Millions of Users. (n.d.). Statista Infographics. https://www.statista.com/chart/2540/data-breaches/

 Kuner, C. (2018). The GDPR as a Chance to Rethink the Paradigm of Data Protection. International Data Privacy Law, 8(1), 3-18.

 Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Newman, L. H. (2018). Now cryptojacking threatens critical infrastructure, too. Wired. Retrieved from www.wired.com/story/cryptojacking-critical-infrastructure/

 Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

 Solove, D. J. (2007). The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. Yale University Press.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.

 World Economic Forum. (2018). Blockchain Beyond the Hype: A Practical Framework for Business Leaders.

 Krawisz, D. (2013, June 24). The proof-of-work concept. <http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/>