OCCASIONAL PAPERS, VOL. 1, NO. 4 - SEPTEMBER 1, 2022

SECURING WEB3
AND WINNING THE BATTLE FOR THE FUTURE OF THE INTERNET

by Charles Clancy, Christopher Ford, Michael D. Norman, and Sanith Wijesinghe

MITRE's Center for Strategic Competition and the "Occasional Papers" Series

Today's competitive strategy challenges are multi-faceted and complex. They exist in arenas of hard, "sharp," and soft power—from military capacity, technological innovation, economic development, espionage, trade, and finance to cyber conflict, law enforcement, politics and culture, and diplomacy. Well-crafted competitive strategy requires a true system mindset.

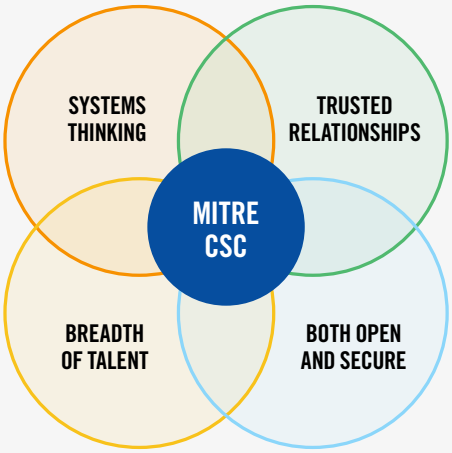
Helping our country meet these challenges drives the work of MITRE's Center for Strategic Competition (CSC). The CSC leverages MITRE's six decades of systems thinking and systems integration experience on behalf of the United States and its partners, drawing upon the full range of capabilities that exist across the MITRE enterprise.

Much of what we do occurs out of the public eye for specific federal sponsors. Because strategic competition is a genuinely "whole-of-nation" challenge, however, it is essential to involve a wide range of stakeholders in devising and implementing systems-informed solutions.

CSC established this "Occasional Papers" series to engage, educate, and inform the policy community and the broader public about strategic competition issues, problems, and opportunities. We invite you to send feedback to strategic.competitor@mitre.org.

Why do we need the Center for Strategic Competition (CSC)?

Understand complex interactions between elements of a system and devise interventions to improve outcomes



Decades of trusted relationships with uniquely broad range of federal sponsors, and in coordinating partnerships among government, industry, and academic stakeholders

Data analytics, economic modeling, AI, behavioral sciences, intelligence analysis, system-of-system modeling, and decision-support tools

Cutting-edge analytic capabilities integrating unclassified and classified information and analyses

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

Contents

Executive Summary

A battle is underway for the future of the Internet, with Chinese technology firms and the Chinese Communist Party actively seeking to dominate ever-larger portions of the world's digital infrastructure and reshape Internet governance around centralized authoritarian models. There may be, however, elegant technical answers to some of these challenges: answers that could permit the next generation of web connectivity to operate in ways that both help catalyze another era of connectivity-facilitated growth and innovation and revolve around decentralized and "democratized" dynamics that would undermine the power and influence of the authoritarian Chinese technology stack.

Web3 is the next generation of the Internet and will bring together new networking technologies and financial infrastructure in a way that blurs the traditional boundaries of telecommunications and finance, creating new decentralized and democratized models of network interaction built around the cryptographically secured autonomy of web users. For this to work, however, these novel web3 technologies need to be made secure against a range of non-state and state-level attackers, and engineering such security into web3 cannot be approached merely as an afterthought.

This paper suggests how to approach the critical task of securing web3 against such adversaries. The web3 threat model must account for efforts to compromise confidentiality, such as mass surveillance by authoritarian governments of their populations' financial transactions, exploitation of web3 infrastructure and services to enable fraud and illicit finance, and attacks against availability that deny or degrade web3 service access. Web3 must be resilient against organized crime and nation-state actors with vast resources and access to infrastructure.

This will require new cybersecurity frameworks, standards, and best practices, and ones that will apply differently to different layers of the emerging web3 ecosystem:

- Blockchain infrastructure entities face both traditional and emerging cybersecurity threats and must securely provision, deploy, and manage their systems.
- Financial services and centralized exchanges should comply with existing cybersecurity requirements for their industry and support existing threat finance requirements, such as know-your-customer (KYC), anti-money laundering (AML), and countering the financing of terrorism (CFT) policies.
- The web3 design must accommodate Decentralized Autonomous Organizations (DAOs), which are unique entities in the web3 space, and will need a growing set of smart contract cybersecurity audit and monitoring services, as well as emerging standards in contract design.
- Endpoint devices and web3 platforms should meet existing web2 cybersecurity expectations.

Advancing the ecosystem further necessitates cyber threat information (CTI) sharing in support of a broader threat-informed defense. Web3-specific extensions to frameworks such as STIX™ and MITRE ATT&CK® can help capture these ontologies. New and existing information-sharing partnerships can then take advantage of these interoperable formats to tackle cybersecurity and financial threats.

As new policy is considered for web3, this paper offers the following specific policy recommendations:

- The National Institute for Standards and Technology (NIST) should develop cybersecurity frameworks, standards, and best practices for web3.
- The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) and the broader counter-threat-finance ecosystem should launch a new public-private partnership for CTI sharing that can help mitigate detrimental security and financial outcomes.
- Regulators and sector-specific agencies should incentivize web3 entities to support and participate in independent performance standards and associated audits covering financial transparency and reliability and cybersecurity, as well as transparent compliance mechanisms across the ecosystem through monitoring and reporting.

For the U.S. government to take a leadership role in the web3 community, it is important to also implement appropriate protections for individual privacy while advancing these security objectives.

Introduction

Given the ways in which the Internet and Internet-enabled applications are intertwined with essentially every aspect of modern life, questions of who controls the Internet and sets the standards to guide its development—or whether it is controllable at all—are of huge significance. This is true, moreover, not only for the prosperity and security of everyone who in the future will rely upon the Internet, but also for the future of geopolitics.

It is not merely that the involvement of Chinese technology companies in providing more and more of the world's digital infrastructure opens the door to Chinese espionage and intellectual property theft. Nor is it only that China's acquisition of a dominant role in other countries' digital networks opens the door to strategic manipulation, giving Beijing the ability "monitor or divert data or even to cut traffic entirely in the event of a conflict,"[1] though these things are certainly true. It is also that the digital technology stack being promoted by state-supported Chinese firms and subsidized by Chinese government loans is itself an inherently authoritarian one, both in its centralized technical architecture and in the broad purposes of social monitoring and control it is designed to facilitate.

The digital networks Chinese firms are building—both in China itself and in parts of the developing world through so-called "Belt and Road Initiative" projects and other efforts—already frequently include design features specifically intended to facilitate government surveillance and control of local populations.[2] China and Chinese firms, moreover, are working to shape the international standards that will govern the future of telecommunications and the development of the Internet in ways that will accentuate the centralized architecture and authoritarian nature of this technology stack. For example they permit system managers to "monitor and gate individual access" to the Internet by every device therein[3] in ways that would "effectively rebuild the technical architecture of the internet to support centralized enforcement and top-down control of information flows within a single country's cyberspace."[4] If such authoritarian standards indeed become the dominant ones for the Internet of tomorrow, and if state-subsidized Chinese firms—which themselves already operate on such a basis and are answerable to and facilitate oppression by the Chinese Communist Party—continue their campaign to colonize more and more of other countries' digital infrastructure, the world would likely become a much grimmer and more repressive place.

THE THIRD GENERATION OF THE WORLD-WIDE WEB, KNOWN AS "WEB3," REPRESENTS A SIGNIFICANT SHIFT FOR THE STRUCTURE AND BUSINESS MODEL OF THE INTERNET.

But there is reason for hope, for these worrying efforts to manipulate the future architecture of the Internet come at a time of great technical creativity and promise. We are today at a point at which the innovations of so-called "web3" technology have the potential to revolutionize the basic architecture of the digital world and help move it in a very different direction: a radically decentralized and potentially powerfully anti-authoritarian direction.

The third generation of the world-wide web, known as "web3," represents a significant shift for the structure and business model of the Internet. Built on top of blockchain technology, web services in this model would be powerfully democratized and decentralized, and users would actually own the infrastructure themselves and pay for services using cryptocurrency. This is a stark contrast to the heavily centralized "web2," in which hyperscalers

monetize user interaction through ads, and would allow a significant "democratization" of actual web activity even if the physical hardware and electronic "pipes" of the system continued to be managed in traditional ways.

But such a revolution in decentralization can only work if web3 can be made secure as a matter of architectural design in ways that the current system is not. And, as with any new generation of technology, web3 has cybersecurity challenges that will need to be overcome. While blockchain provides a unique security building block, vulnerabilities are likely to abound in higher layers, particularly as innovators rapidly build out the ecosystem. Given the direct connection between cryptocurrency and web services, hackers have special motivation to defraud the system.

For web3 to live up to its potential and for these novel technologies to provide a new, decentralized model of web activity, these and other problems will have to be solved. This paper provides an overall framework for securing web3—in particular, for combatting fraudulent, illicit, and disruptive exploitation of web3-based cyber vulnerabilities—and seeks to inform emerging U.S. policymaking in this arena to help ensure that an American-led web3 ecosystem gets ahead of potential security vulnerabilities and provides a stable engine for economic growth and technological innovation.[5] It builds on our prior call to action for a national strategy in web3,[6] which provided a more detailed introduction to web3 technology and how the Internet has evolved over the past 40 years.

Threat Model

Securing any complex system requires an understanding of the adversary, and different types of adversaries are likely to present different sorts of challenge. To design an effective security architecture for web3, we must make assumptions about the technical means and motivations of such adversaries. The table below thus summarizes three classes of adversaries: the *spy*, the *thief*, and the *disrupter*. These categories respectively align with the familiar security triad: Confidentiality-Integrity-Availability.

ADVERSARY CLASS	DESCRIPTION
The Spy	Transactional intelligence can be extraordinarily valuable to industrial competitors, authoritarian governments, law enforcement agencies, financial regulators, and spy agencies. Different blockchains have different approaches to privacy, and the balance between transparency and privacy is nuanced. In general, we seek to minimize mass surveillance to protect civil liberties, while enabling lawful access to data for legitimate purposes.
The Thief	Web3 is based on tokens that have market value, whether they are a cryptocurrency or some other form of digital asset. This motivates a class of adversaries who seek to defraud the system and steal these assets. Fraud can come in many forms, from scams catalyzed by a highly speculative market to exploiting logic bugs in smart contracts. In general, we seek to combat fraud by closing digital loopholes and empower law enforcement and regulators to hold accountable those who perpetrate scams.
The Disruptor	Disruption and denial are often wartime objectives that can be achieved just as easily with a cyber attack as a munition. In an era of strategic competition with countries like China and Russia, such actions could be taken outside a declared war as an instrument of economic or information power. Similarly, terrorist groups could target digital infrastructure. In general, we seek to build resilience into our systems that makes it incredibly difficult to disrupt web3 infrastructure or deny access to it.

Within each motivational class, there are a range of capabilities or access that an adversary may have. Criminal organizations and nation-state actors, for instance, generally have significantly more resources than individual hackers. Insider threats may have unique insights and accesses. To be secure, we should design systems to be secure against all these threats.

Accomplishing all these security goals in web1 or web2 technology is tremendously difficult—arguably impossible. However, web3 has a trick up its sleeve. Building on top of a decentralized blockchain provides two new fundamental security properties to the transactional layer of the Internet: Byzantine fault tolerance and non-repudiation. This guarantees, generally, that unless an adversary can compromise more than half the cyber infrastructure, it cannot create, destroy, or alter Internet transactions.

However, as a recent Defense Advanced Research Projects Agency (DARPA)-funded report by Trail of Bits notes, blockchains must be truly decentralized for these security properties to hold, and often the underlying infrastructure is not as decentralized nor as secure as users assume.[7] A wide range of attacks are possible against the technology that underpins web3.

Cybersecurity Framework and Standards

Like any critical infrastructure, the starting point for security is frameworks such as the NIST Cybersecurity Framework.[8] Arguably the decentralized nature of web3, and the way in which services are architected and delivered, complicate direct application of the NIST framework, which generally assumes asset-owner operators control vertically integrated infrastructure. By contrast, web3 is horizontally integrated with different entities providing different layers of service. A unique challenge is that in web3 some of those layers may be DAOs, operating as smart contracts within a blockchain, without a board of directors or management team.

Consequently, we will need a new cybersecurity framework for web3. New cybersecurity best practices, guidelines, and standards are needed for each different class of web3 entities.

Infrastructure Entities

As pointed out by the Trail of Bits report, the infrastructure that underpins web3 is vulnerable. This includes mining (proof-of-work blockchains) and staking (proof-of-stake blockchains) validator nodes. These devices are run by people who receive micropayments per transaction as compensation. Often, they are organized into collectives that pool fees and distribute them across the collective.

Securing infrastructure entities involves:

- ensuring the hardware/software stack for infrastructure nodes is locked down and secure, with up-to-date software and patches, secure provisioning, and robust access control;
- requiring that blockchain software running on nodes is up to date, running the latest version of the relevant codebase;
- implementing denial-of-service protection against network-level attacks that seek to degrade network performance; and
- developing security best practices for cross-blockchain bridge architectures; and to the extent possible, incentivizing continued decentralization at multiple scales.

Mining and staking pools have a unique responsibility to ensure the security of the infrastructure and are major players in these ecosystems. Both the operators and members of a pool should have sufficient financial incentive to self-regulate the security of the infrastructure under their members' management. Additional disclosure rules that require investors be given visibility into infrastructure standards compliance can also help drive adoption of best practices to mitigate detrimental outcomes.

Financial Institutions and Centralized Exchanges

With the growth of Decentralized Finance (DeFi), financial institutions and centralized exchanges have become major pillars in the web3 ecosystem. They are the primary interface for users interacting with and trading cryptocurrency. They are on the front lines of implementing current financial regulatory requirements, including AML, KYC, and CFT.

Security for this portion of the ecosystem includes:

- compliance with existing financial institution security requirements, such as the Payment Card Industry Data Security Standard;[9]
- compliance with financial regulatory requirements such as AML, KYC, and CFT;

- active programs to proactively work with relevant law enforcement agencies in tracking down fraudulent or illicit financial activity transiting web3 infrastructure, such as ransomware payments; and
- implementation of tools that make it easy for users to comply with compliance regimes, such as taxation.

Beyond compliance with existing security and financial regulatory requirements, key to securing this portion of the ecosystem is automating data sharing, as described further in Section 4.

Decentralized Autonomous Organizations

DAOs are an entirely new type of ecosystem player for which we lack analogs and precedent in prior generations of Internet and financial infrastructure. Built as smart contracts resident on a public blockchain, DAOs generally have no board of directors or management team, making decisions through either prescribed algorithmic rules or democratic voting by holders of special governance tokens.

To date there have been a wide range of hacks against DAOs that fall into different classes:

- **Flawed code** – Smart contracts are software, and bugs in the underlying code can be manipulated by hackers to steal DAO assets or prevent legitimate users from withdrawing them.[10]
- **Vote bribing** – Often associated with Sybil attacks, bad-faith actors "may use flash loans or other DeFi primitives to borrow an effective majority of voting tokens on the open market in order to use those votes to send DAO-controlled assets to themselves, such as the recent Beanstalk hack.[11]
- **Decentralized control weakness** – DAO treasuries, while appearing to be controlled by democratic voting processes, may at times be multi-signature wallets to which a small number of insiders are afforded signing privileges. Those controlling these treasuries may act according to democratic will, until such time that a decision no longer serves their personal interests. This weakness is worsened by off-chain voting, which seeks to achieve more-equitable participation by removing the sometimes-expensive fees associated with on-chain voting.

Given the potential financial loss, a myriad of smart contract security services have emerged over the past few years. From software frameworks that make it easier to design secure smart contracts, to code analysis tools that look for logic flaws in smart contract code bases, developers of smart contracts have a rapidly-evolving set of tools at their disposal. Other than those engaging in fraudulent activity, groups developing and deploying DAOs should increasingly have a financial motive to employ these tools, but with new oversight anticipated from the Securities Exchange Commission (SEC) and/or Commodity Futures Trading Commission (CFTC), there could be new regulatory hooks to incentivize use of these services.

With respect to vote bribing, there are several proposed solutions, including quadratic voting, that make it more difficult to undermine the democratic will of a DAO's membership. These should be employed by DAOs. Modeling and simulation may provide avenues for designing more-resilient governance, and decentralized identity solutions may be required to push beyond purely plutocratic control mechanisms.

At least one prototypical end-to-end solution to the control weakness problem is available (i.e., Gnosis SafeSnap,[12] which combines a Gnosis Safe with Snapshot off-chain voting), but standards are virtually nonexistent. The solution space here revolves around using smart contracts to cause off-chain voting to trigger the disbursement of treasury funds such that all humans are removed from the post-vote control process.

Interaction Layer and Endpoint Devices

The blockchain is a record of transactions that we collectively believe are true. Interacting with that data requires some sort of web-based platform such as OpenSea (digital art), Cloutfeed (decentralized social media), or Decentraland (metaverse). The interface layer is important from a security perspective because of its ability to render blockchain data in a misleading or fraudulent way.

From a security standpoint, this layer should strive to at least meet the cybersecurity levels employed by web2 platform companies, though unfortunately, outside federal government regimes such as FedRamp, there is no commonly agreed upon set of security best practices for web2. Larger questions about censorship and freedom of speech, and obligations for these platforms to provide transparency, remain. It remains to be seen how free-market pressures translate into the emergence of competing interface platforms mapped to the same underlying blockchain data. In principle, given that the underlying data is public, there are low entry barriers to new entrants that can help drive competition for value-add services and protections.

Similarly, endpoint devices will be critical to this ecosystem, including things such as smartphones, computers, and hardware digital wallets. Significant digital-asset theft happens today by phishing end users and compromising their crypto wallets or exchange credentials. Current consumer cybersecurity best practices must continue to apply to these devices, whether interacting with web2 or web3 services.

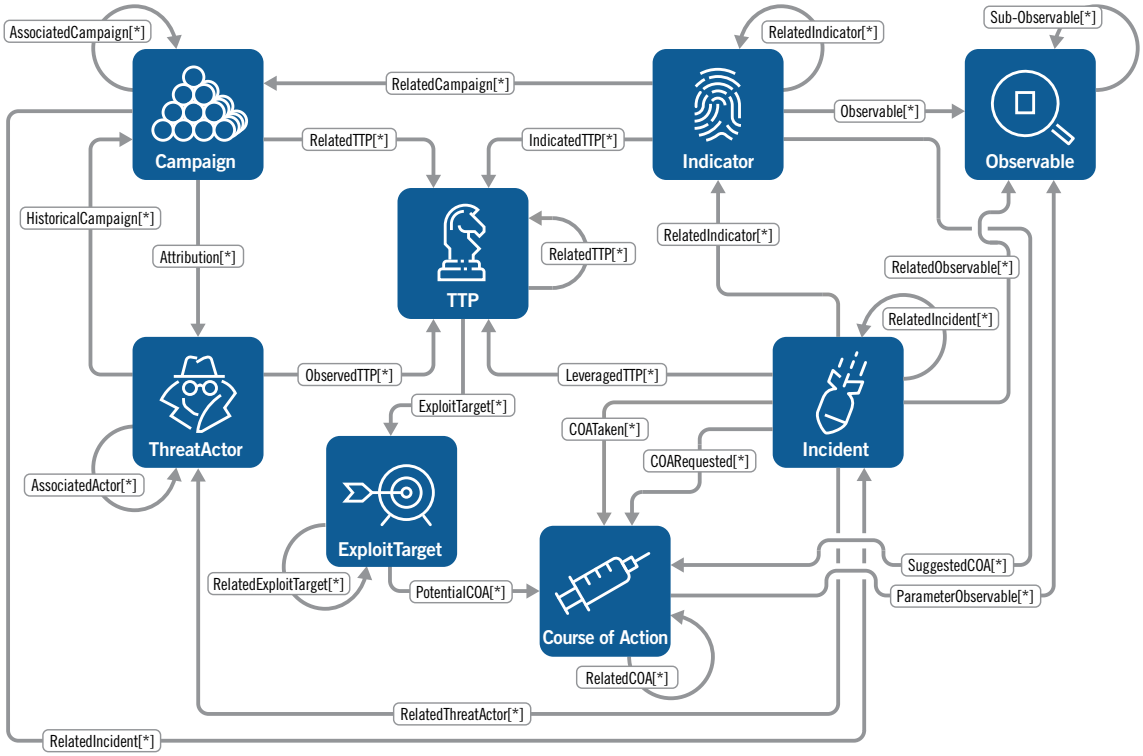


Figure 1. Diagram of the STIX taxonomy (https://stixproject.github.io/about/)

Threat Informed Defense and Information Sharing

Given the scale and complexity of the cyber threat, an important part of the solution space is to take a threat-informed approach to defense. This concept was pioneered by the MITRE ATT&CK framework and has been broadly applied to the security industry.[13] Key to implementing a threat-informed defense across a technology ecosystem is real-time information sharing.

Threat Informed Defense for Web3

Building out a threat-informed defense ecosystem for web3 necessitates a full taxonomy of the unique threat surface for web3 infrastructure, institutions, and services. The current vocabulary within frameworks such as MITRE ATT&CK can accommodate many of the information technology and cloud aspects of web3, but likely unique indicators will be needed for things like blockchain nodes and wallet identifiers. From this we can then identify and classify tactics, techniques, and procedures (TTPs) for a new class of threat actors, based on observed hacks against web3. MITRE plans to further develop ATT&CK for web3 over the next year and make it available to the broader cybersecurity community. Additional efforts to create a cyber range and test harness for web3 infrastructure are also under consideration.

The ecosystem of CTI for web3 is more diverse than our current vocabulary. For example, one approach to implementation is extending Structured Threat Information Expression (STIX), shown in Figure 1 , which currently targets more-traditional Internet technology. The STIX taxonomy likely needs extension in the following ways:

- Rather than IP and email addresses, the building blocks for web3 are **observables**, such as wallet identifiers and Ethereum Node Records.
- **Indicators** now include things such as blockchain transactional records between entities such as user interaction with DAOs.
- **Incidents** can include not only traditional cyber exploitation and attack but also illicit, fraudulent, or bad faith financial transactions.

Cyber Threat Information Sharing for Web3

With frameworks like STIX and ATT&CK extended to support the vocabulary of the web3 threat surface, we can share CTI. Typically, such sharing occurs through trusted intermediaries, such as Information Sharing and Analysis Centers (ISACs).

Within the web3 ecosystem there are many stakeholders, with the following being a couple examples of key organizations working on cybersecurity or financial crime issues:

- **Communications ISAC**: Run by the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security (DHS)
- **Financial Services ISAC**: The largest and most mature of the ISACs, the FS-ISAC brings together financial services companies in 70 countries with the Financial Services Sector Coordinating Council and U.S. Treasury Department.
- **FinCEN**: Housed within the U.S. Treasury Department, FinCEN collects and analyzes transactional financial information, to combat fraud and illicit finance.

It is unlikely that a single information-sharing ecosystem will exist for web3, given the heterogeneity of ecosystem players and range of use cases (e.g., cyber crime versus financial crime). However, if a common language is developed for players to communicate in a machine-to-machine fashion, then it will support the necessary lattice of organically developed trust groups, analysis organizations, and threat feeds.

Policy Recommendations

This section summaries a few key policy recommendations that can help energize the web3 cybersecurity community and get the ecosystem started off on the right foot.

Recommendation 1: Develop cybersecurity frameworks, standards, and best practices

NIST should develop a detailed cybersecurity framework for web3 technologies that focuses on building, deploying, and operating various aspects of the web3 stack.

NIST should develop standards for cybersecurity of blockchain infrastructure, through its Special Publication 800-series.

Through the National Cybersecurity Center of Excellence, NIST should partner with industry to prototype current and emerging web3 use cases and develop best practice guides for their secure deployment and operation.

The NIST Privacy Framework should be extended to include guidelines on implementing decentralized identity protocols that allow citizens to port their identity credentials across application service providers and mitigate theft of personally identifiable information from security breaches.

Recommendation 2: Establish FinCEN threat-sharing partnership

The U.S. Treasury Department's FinCEN, in partnership with relevant federal law enforcement agencies, the Office of Cybersecurity and Critical Infrastructure Protection, and financial regulators, should launch a new public-private partnership focused on building out the CTI sharing ecosystem for web3, including both the cybersecurity and financial crimes aspects. This new partnership should work closely with the relevant ISACs and other stakeholders to develop the data sharing standards, processes, and tools to support real-time sharing and analysis of web3-related CTI. Opportunities to engage with international law enforcement agencies should also be explored here to help address the transnational dimensions of the threat landscape.

Recommendation 3: Incentivize cybersecurity audits and compliance

DHS, in partnership with the Department of the Treasury, should develop a program to monitor infrastructure security for major blockchains and core web3 infrastructure. By publishing this data, infrastructure operators can be motivated to ensure their systems are up to date and secure.

As the CFTC and SEC pick up the regulatory reins for the cryptocurrency infrastructure within web3, they should incentivize normalization of smart contract security auditing by requiring it as part of mandatory disclosures and periodic reporting.

Regulated entities under CFTC and SEC should be covered entities under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and be required to report breaches.

Conclusion

Security is very difficult to engineer into a system *after* the fact, particularly as authoritarian regimes seek to build vulnerability in from the start. Injecting democratic values into new technologies requires that we protect users from criminal scams, cyber espionage and intellectual property theft, authoritarian surveillance, and strategic coercion by hostile regimes. But the struggle for the future of tomorrow's Internet is not yet over; indeed, in technical terms, it has barely begun.

If we can do more to engineer security into the web of tomorrow by securing web3 against the range of challenges and deliberate assaults that it will inevitably face, we will position it for success as a powerful tool of economic growth and innovation, while simultaneously making life much more difficult for the criminals, cyber spies, and authoritarian regimes that seek to exploit or co-opt modern connectivity for their own purposes. This paper has offered some suggestions about how to achieve such security. The time to start is now.

About the Authors

Charles Clancy is a senior vice president at The MITRE Corporation, general manager of MITRE Labs. He previously served as MITRE's vice president for intelligence programs and before that as the Bradley Distinguished Professor in Cybersecurity at Virginia Tech and Executive Director of the Hume Center for National Security and Technology.

Christopher Ford is a MITRE Fellow and directs the Center for Strategic Competition. He served until January 2021 as U.S. Assistant Secretary of State for International Security and Nonproliferation and also fulfilled the duties of the Under Secretary for Arms Control and International Security.

Michael D. Norman is a principal systems engineer at MITRE and the web3 and digital assets capability area lead. He has worked in decentralized systems and cryptocurrency for the past 17 years and holds a doctorate in complex systems and brain sciences from Florida Atlantic University.

Sanith Wijesinghe is a technical fellow at MITRE and works at the intersection of financial infrastructure and technical innovation. Before joining MITRE in 2011 he spent seven years as a technologist on Wall Street.

Acknowledgements

The authors would like to thank the following individuals for their thoughtful input and review: Emily Frye, Kevin Toner, Craig Wiener, and Ryan Farley.

Endnotes

1 Telecommunications equipment and services provided by the Chinese company Huawei, for instance, have been associated with apparent espionage activity in locations as diverse as the Netherlands and Ethiopia. See, e.g., Jonathan E. Hillman, The Digital Silk Road: China's Quest to Wire the World and Win the Future (New York: Harper Business, 2021), at 14 & 68; Ghalia Kadiri & Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionnépar Pékin," Le Monde (January 26, 2018), *available at* https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; Jonathan E. Hillman, The Emperor's New Road: China and the Project of the Century (New Haven: Yale University Press, 2020), at 188-89.

2 *See*, e.g., Hillman, The Emperor's New Road, *supra*, at 187-88 (discussing ZTE networks constructed by ZTE for the Ethiopian government).

3 Elizabeth C. Economy, The World According to China (Cambridge: Polity Press, 2022), at 198.

4 *See* U.S.-China Economic and Security Review Commission, 2020 Report to Congress, 116th Congress, 2nd Session (December 2020), at 111, *available at* https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf.

5 This paper does not address the broader questions of financial and economic resilience associated with cryptocurrency and decentralized finance.

6 Charles Clancy, "Call to Action: Developing a National Strategy for Web3," MITRE Corporation (March 2022), *available at* https://www.mitre.org/publications/technical-papers/call-to-action-developing-national-strategy-web3

7 Evan Sultanik et al., "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers," Trail of Bits (June 2022), *available at* https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf.

8 National Institute of Standards and Technology, "Cybersecurity Framework" (undated), *available at* https://www.nist.gov/cyberframework.

9 *See* PCI Security Standards Council, "PCI DSS v4.0 Resource Hub" (undated), *available at* https://www.pcisecuritystandards.org/

10 @vaibhavsaini_67863, "HackPedia: 16 Solidity Hacks/Vulnerabilities, their Fixes and real world examples" (July 21, 2018), *available at* https://hackernoon.com/hackpedia-16-solidity-hacks-vulnerabilities-their-fixes-and-real-world-examples-f3210eba5148

11 Corin Faife, "Beanstalk cryptocurrency project robbed after hacker votes to send themself $182 million," The Verge (April 18, 2022), *available at* https://www.theverge.com/2022/4/18/23030754/beanstalk-cryptocurrency-hack-182-million-dao-voting

12 *See* https://docs.snapshot.org/plugins/safesnap.

13 *See* MITRE Corporation, ATT&CK website, *available at* https://attack.mitre.org/

MITRE

SOLVING PROBLEMS
FOR A SAFER WORLD®