Communities, Agency, and Resilience: A Perspective Addressing Tragedy of the Cyber Commons

Samir Jarjoui
Dr. Renita Murimi
Robert Murimi

ABSTRACT

Cybersecurity suffers from a "tragedy of the commons" problem, where people and institutions have adopted lax security practices due to a tendency to weigh the perceived costs of adopting sound cybersecurity practices as higher than their expected benefits. For example, despite advancements in cybersecurity measures and extensive investments in tools and strategies to counter cyberattacks, foundational best practices have faltered leading to global cybersecurity challenges. Part of the dilemma stems from the fact that cybersecurity continues to be approached with a limited mindset, which creates a significant threshold of social cohesiveness for combating cyber threats. In the meantime, the cyber threat landscape continues to proliferate and exploit the fragile networks that we all inhabit. This paper provides a community-centered framework for cyber resilience that offers a starting point for addressing the tragedy of the commons problem in cybersecurity.

INTRODUCTION

Who is responsible for cybersecurity? From a proactive stance, people have assumed that the responsibility of cybersecurity lies under the purview of "others," a loose category encompassing the information technology teams, services teams, cloud providers, administrators, vendors, clients,

Samir Jarjoui is the Director of IT at Herb Pharm. He has 15 years of experience in IT management, cybersecurity, internal audit, and risk management. His work focuses on business and IT alignment to optimize organizational capabilities. He holds several professional certifications in the field of cybersecurity and a DBA with a focus on cybersecurity from the University of Dallas. He is also an adjunct professor of business at Warner Pacific University.

and a plethora of other stakeholders. From a reactive stance, as in the aftermath of a cybersecurity incident, we have resorted to shifting the onus of responsibility onto "others," assuming that someone else should have done better and prevented the cybersecurity incident from happening in the first place. This is similar to the problems surrounding climate change, where people all over the world have consumed natural resources without regard for consumption's wider effects, leading to poor environmental conditions for all of us. This situation was termed the "tragedy of the commons" by ecologist Garrett Hardin in his 1968 article referring to the adverse effects of overconsumption of scarce common resources.[1] In the context of environmental stewardship, the tragedy of commons (ToC) problem refers to finite environmental resources that risk being driven to empty when faced with users who over-consume them. Thus, a finite resource faces over-usage by individual actors who discount the impact of their usage patterns on the sustainability of the finite resource for the rest of the actors and for future generations.

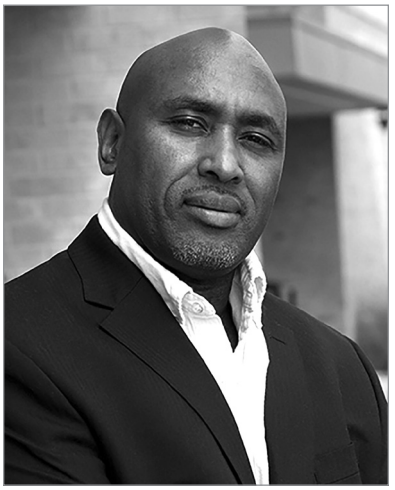
In the context of cybersecurity, however, we suggest that there is no single finite resource that is being driven to extinction. Cybersecurity is not a finite environmental resource like clean water or air. However, the resources to create, maintain, and sustain the security of our networks and data are finite. There are four kinds of resources used in cybersecurity that are closely interdependent. First, monetary resources that govern the investments made in cybersecurity infrastructure are limited, due to the finite nature of budgets where the return on investment for cybersecurity expenses is not easily quantified. Second, the hardware and software tools required to secure networks (whether cloud-based or physical infrastructure) are constrained by various factors related to the spatial needs of organizations and the associated monetary constraints. Third, the field of cybersecurity expands rapidly due to continuously emerging threats

Renita Murimi (IEEE SM'21) received her PhD and MS in Electrical Engineering from New Jersey Institute of Technology, and a Bachelor of Engineering in Electronics and Communications from Manipal Institute of Technology in India. She is an Associate Professor of Cybersecurity at the University of Dallas. Her current research interests are in the areas of cybersecurity and network science.

from a multitude of attackers with varying levels of resources. The continuous learning involved in staying abreast of recent challenges and developments of countermeasures pose significant temporal and cognitive constraints on the ability to defend our networks and make them resilient when attacked. Finally, the field of cybersecurity is characterized by substantial constraints in recruiting a qualified workforce. The talent shortage in cybersecurity has created a supply-demand gap in the cybersecurity workforce that leaves positions vacant as threats continue to proliferate. The commons of cybersecurity, thus, are the resources required to protect cyberspace from adversaries.

Much has been written about whether the Internet or the cyberspace constitute commons at all. Digital commons have been analyzed in the context of cyberspace freedoms,[2] the electromagnetic spectrum,[3] and in the context of the generation of data, information, culture, and knowledge.[4-6] The ToC problem was also studied in the context of online consumer communities, where user tendencies to free ride instead of contributing were identified as a challenge to the sustainability of the commons.[7] Other forms of the digital commons have been conceptualized, including social media commons,8 open-source software commons,[9] bandwidth and information commons,[10,11] and the commons of public trust that users place in cyberspace.[12] Simultaneously, previous research has refuted the notion of the Internet as commons by arguing that the Internet is neither "exclusionary nor rivalrous," and hence does not qualify as a commons.[13] Dan Hunter proposed that the Internet is a digital anti-commons, wherein private ownership of different kinds of online resources (licenses, permissions, and copyrights) prevents others from optimally using the resource.[14]

Over the years, the unrelenting pace of cyber incidents is a stern reminder of the inadequacies of current cybersecurity solutions. Furthermore, in technologically advanced societies, cyber threats are often



Robert Murimi received his MS in Computer Engineering from New Jersey Institute of Technology and a BS in Computer Science from New Jersey City University. Currently, he is pursuing a DBA with a focus in cybersecurity from the University of Dallas. He has over fifteen years of experience in software development, and is currently a software engineer at McKesson.

magnified by additional challenges such as antiquated, strained, and complex critical infrastructure systems, further complicated by the vast interconnectivity of many global communication systems.[15] We argue that it is time for a new approach to address the root causes of ToC in cybersecurity, one that can be tailored to building cyber-resilient communities to deal with evolving threats. People are quick to dismiss their role in protecting their networks and data, often relying on ignorance, or a tendency to underestimate the impact of their inadequate efforts, or a dependence on "others" to play their part in cyber security. The often-used aphorism of "it is not a question of whether, but when we will be hacked" points to a reluctant acceptance of the notion that nothing can be done to protect oneself in the cybersecurity war. Thus, a different ToC has unfolded in our digital environments, one where the impact of one's actions is not fully understood, and so the operational attitude is to resign to the occurrence of the inevitable breach or wait for "others" to do something to contain the fallout. ToC, thus, is a driving factor in the challenges to cyber defense that confront our fragile networks, where threat actors can advance their strategic and geo-political interests by furthering information warfare.

We see hope in a radical solution for ToC, of the kind that Elinor Ostrom proposed when she suggested that regulation was not the only way to proceed when it came to climate change.[16] Her work, eventually leading to the 2009 Nobel Prize in Economics, studied how small, stable communities under certain conditions manage their local common resources without falling victim to the ToC tragedy. A similar mindset could be utilized to adapt Ostrom's approach to ToC in cybersecurity. Ostrom's approach to addressing the ToC problem helped shift the focus away from top-down governance and regulatory approaches as the only mechanism to address the ToC problem. Her grassroots, bottom-up approach was proposed as a

supplement to regulation, and not a superior approach to regulation. Thus, her approach for cooperative institutions that were organized and run by the users of the resources brought a new approach to the field of commons management as a whole. Ostrom's approach has led to the formation of design principles that were influential in the management of common pool resources, from which sound inference about commons and their management for diverse applications can be made.

In this article, we propose a systems approach[17] to develop cyber-resiliency for transcending the ToC problem in cybersecurity. Our solution framework outlines three dimensions—innovative learning, awareness, and adaptability—as the essential foundation for cyber-resilient communities who can effectively anticipate risk, mitigate deficiencies, and recover from inevitable cyberattacks. We believe our framework can help accelerate the emergence and sustainability of cyber resilient communities, who in turn can influence the development of new communities to reach a magnitude and intensity that overcomes the problem of ToC in cybersecurity. In the next section, we outline the need not just for cybersecurity, but for a broader goal of cyber resilient commons.

The Need for Resilient Commons

Resilient cyber communities go hand in hand with resilient cyber commons. Resilience requires a rapid restoration of resources and proactive efforts that begin with acknowledging the inherent risks to the resources. Cyber attacks are characterized chiefly by an asymmetric distribution of information. This asymmetry extends to various facets of cybersecurity. When cybersecurity countermeasures that are deployed to thwart attacks work efficiently, the defenders have the upper hand. Conversely, when these measures fail, the attackers have the upper hand. The sophistication of the attacks points to an asymmetric distribution of resources and accountability for attackers. This is because for attackers it is enough to launch a successful attack only once, but defenders have to be on guard all the time.

The lack of standardization in cybersecurity defenses also leads to a variety of cybersecurity postures adopted by individuals and organizations. This asymmetry in cybersecurity postures makes it easier for attackers to go after organizations with weaker deterrence initiatives. Further, there is asymmetry involved in the accountability assigned to attackers and defenders. In certain kinds of cyber attacks such as denial-of-service attacks, when an individual's or an organization's network is attacked, the response to the attack involves network redesign or network repair, both of which are resource-intensive efforts without any immediate payback for the attacker. In other kinds of attacks such as ransomware attacks, if the victim does not pay the ransom, the attacker does not receive the ransom but still has access to the exfiltrated data from the ransom attack. For example, when a hacker group breaches a network or an individual account, the victims are not able to hold the attackers responsible or launch counterattacks to deter them. Thus, intrusions can't be matched with counter-intrusion, unless external forces such as governments and political institutions intervene. Typically, such

interventions are reserved only for highly disruptive attacks motivated by overt geo-political tensions. This asymmetry of attacker resources, attack vectors, and attack outcomes creates a disjointed cybersecurity landscape, where individuals and organizations find it more convenient to resort to the ToC mode of operations rather than explore multidimensional solutions that go beyond technological countermeasures. The past few decades have shown us that an effective cybersecurity strategy is a proactive one that allows for continuity and restoration of operations when faced with an attack, creating resilience in our digital infrastructure.

In general, resilience refers to the ability to adapt in a positive manner despite experiencing adversity.[18,19] Resilient systems can transcend changes and disturbances while retaining the same essential structure and capacity.[20] Existing literature on cyber resilience has risen out of the experiences and challenges of implementing cyber resilience within specific application domains. Cyber resilience lies at the intersection of several interconnected business and technology processes, such as supply chain,[21-23] critical infrastructure,[24-26] cyber physical systems,[27-29] and the financial sector.[30] As cyber resilience continues to gain prominence, organizations such as MITRE and NIST have developed extensive frameworks to design, execute, and assess cyber resilience within organizations.[31] Other significant frameworks and metrics include the World Economic Forum (WEF)'s cyber resilience framework, the Department of Homeland Security (DHS)'s Cyber Resilience Review, and the Software Engineering Institute's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and CERT-Resilience Management Model (RMM) frameworks.

Our article is the first to suggest that cybersecurity suffers from the ToC problem, whose solution lies not just in technological but socio-technical approaches to understanding the impact of our actions in our networks. Below, we outline a community-centered framework for cultivating cyber resilience which includes the attributes of innovative learning, awareness, and adaptability to address the root causes of ToC in cybersecurity holistically. The next section describes our motivation for a community-centered framework for developing cyber resilience.

THE MOTIVATION FOR A COMMUNITY-CENTERED FRAMEWORK IN CYBER RESILIENCE

ToC, at its core, is a problem that affects entire communities – here, we use the term "community" rather loosely. As such, solutions that address ToC – whether in environmental stewardship or in cybersecurity – are best designed with an emphasis on communities. In this context of cybersecurity commons, a community could refer to a group of individuals or organizations that use a certain portion of cyberspace or an online network. This description of a community affords flexibility of scale, since networks and subnetworks could be differentiated into various levels of hierarchical online communities. Thus, a community could be the groups of Computer Science students at a college who receive university communications through a learning management system, or residents of a town who receive water and trash utilities, employees of an organization online social network groups, or any other configuration

of online networks and their users. An analysis of the root causes of ToC in cybersecurity points to the following three main themes that inhibit effective cyber resilience – i) superficial cyber resilience approaches ii) failure to reach a tipping point, and iii) lax cybersecurity efforts, as described next.

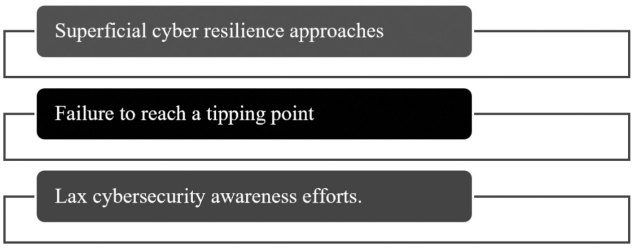


Fig. 1. Categories of challenges to cyber resilience

Superficial Cyber Resilience Approaches

An examination of well-established cyber resilience publications shows that cyber resilience initiatives have been primarily conveyed as a derivative of traditional cyber risk management and incident response strategies. For example, mainstream and prominent cybersecurity advocates, which includes organizations such as the MITRE, National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO), continue to leverage a commonly used set of principles for cybersecurity risk management and cyber resilience artifacts, which typically include the general categories of assessment, detection, response, and recovery.[32,33] In addition, the overlap between cybersecurity and cyber resilience approaches has not been well defined and it is not clear how the two fields complement one another to optimize outcomes.

Further, while cybersecurity has benefited from existing and traditional risk management methodologies, social and cultural considerations continue to be a missing component in most existing strategies for combating cyber threats.[34,35] Without such multi-dimensional considerations, cybersecurity investments and efforts fail to generate the level of engagement needed to influence citizens on a global scale, thereby failing to solve the cybersecurity ToC problem.

Failure to Reach a Tipping Point

Cybersecurity investments continue to increase exponentially at the organizational and governmental levels, but cyber behavior lags behind despite best practices and threat intelligence warnings.[36,37] The actions of individuals can have profound implications, as demonstrated by the case of phishing attacks that require a few or even one compromised account to serve as an entry point for malware. Thus, despite existing efforts and the emergence of cyber resilience as a top priority for cybersecurity practitioners,[38] cybersecurity efforts have so far failed to reach a "tipping point" that enables transformation in cyber behavior at the global level.[39] Individual users' weak cybersecurity practices coupled along with network security flaws are two critical areas that offer areas of improvement for reaching a "tipping point" in security of the cyber commons.

Tipping points occur when a series of small changes become significant enough to propel a system beyond a certain threshold into a new state.[40] Malcolm Gladwell describes various examples, such as fashion trends and social behavior, where small initial changes started a runaway process causing significant transitions.[41] This is the kind of runaway process we are advocating in this research: the ability to generate sufficient and sustainable collective momentum to reach a tipping point for responsible and mindful cybersecurity behavior. The failure to reach a tipping point also derives from the fact that cybersecurity efforts continue to be a top-down approach – initiated, organized, pushed, and managed by governments and institutional bodies with little to no engagement from individual users and communities.

Lax Cybersecurity Awareness Efforts

Due to the rapid evolution of information systems and interconnected communication devices, the Internet has become a significant part of individual's lives. It is, therefore, imperative to cultivate a sense of awareness as a foundation to address the evolving cyber threat landscape. Such awareness is crucial to developing and maintaining cyber resilience, which entails the ability to transcend destructive cyberattacks and involves a certain level of security mindfulness to stay on course.[42]

Current cybersecurity approaches continue primarily to emphasize action-based efforts as information systems-centric measures, and do not frame awareness as a fundamental principle for combating cyber threats. In addition, many cybersecurity awareness training programs continue to fall short due to their misaligned objectives and foci.[43] While the importance of security awareness training has been widely recognized, awareness training programs need to evolve past being merely a "check-the-box" exercise. Awareness efforts need to transform into an emphasis on security mindfulness – changing the "DNA" of communities to produce responsible and security-conscious citizens. The dimensions of the proposed framework's cyber resilience are discussed in the next section.

OUR PROPOSED FRAMEWORK

A community-centric approach to cybersecurity differs from the many traditional approaches to cybersecurity. On one end of the spectrum, a traditional top-down approach neglects to consider the perspectives of stakeholders and communities that are impacted by the choice of cybersecurity policies and tools. A traditional ad hoc approach lies on the other end of the spectrum, where the cybersecurity initiatives that are adopted are mostly reactive, creating a patchwork of solutions that are redundant in some areas and leave coverage holes in other areas. The connectivity of our networks creates fertile conditions for attacks to spread laterally and vertically, mimicking the spread of diseases and epidemics through populations. However, while approaches such as herd immunity offer notable benefits to communities, our digital networks cannot be protected based on herd immunity. In a network of "n" devices where "n-1" devices are protected by strong countermeasures and the

remaining device is unprotected or weakly protected, that one unprotected or weakly protected device poses a significant threat to the security of the network. This single device is merely an example, and can be replaced by any of the following without loss of relevance: a weak link, poorly configured software, open port, lax firewall rule, successful phishing attempt, weak password, expired antivirus software, backdoor, or any of the countless ways that attackers exploit networks. The aforementioned list is only a list of flaws in the technologies, and does not even account for disruptions in the socio-technical, economic, geo-political, and environmental realms.

A community-centric approach to cyber resilience is built on a foundation of trust.[44] In the context of a community approach to security of the cyber commons, trust is an outcome of the shared sense of community responsibility. Such an approach requires that individual and organizational stakeholders work to elevate the cybersecurity posture of all entities, even at the cost of potential short-term gains. For example, in 2016 the Dutch government adopted a policy that increased the encryption capabilities available to users.[45] Such an approach meant that the Dutch government would potentially face situations where they might need access to some information that was encrypted, but would be locked out of access to that information. The Dutch government's commitment to upholding encrypted communication for confidentiality and integrity is evident in their funding of OpenSSL which is an open-source implementation of Secure Sockets Layer (SSL) and Transport Layer Security (TLS)). Their motivation for supporting encrypted communication is in the interests of "fundamental rights and freedoms as well as security interests and economic interests." Another example of a trust-based approach to cybersecurity is that of organizations that reveal zero-day vulnerabilities and report all discovered bugs. It might be costly to engage in such efforts, especially when the secret hoarding of flaws might result in future leverage against competing organizations or nation states. But such myopic activities are detrimental to building cooperation and ensuring the maintenance of trust among stakeholders, keys to the community-centric approach.

One approach to a community-centric approach to cybersecurity is the National Cybersecurity Strategy released by the United States White House in March 2023. This strategy is based on five pillars: defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals. A common theme across these five pillars is the need for "stakeholder communities" in each of these pillars to collaborate for defending cyberspace. A different example of a community-centric approach to cybersecurity is the Japanese Cybersecurity Strategy passed by the National Center for Incident Readiness and Strategy for Cybersecurity (NISC).[46] Among other notable aspects, this strategy specified that all stakeholders (individual, civic, government, companies) were responsible for the security of cyberspace and pointed to participation in information sharing as a prerequisite for a holistic cybersecurity strategy. Additionally, cooperative efforts and alliance building, both international and domestic,

were highlighted as key to building confidence and trust in strengthening Japan's own cybersecurity posture while also strengthening that of its partners. The cross-community collaboration programs, the strengthening of local communities and small and midsize enterprises (SMEs), and adopting this approach in multiple layers starting with the local community and leading up to the international community all characterize the community-based nature of the NISC's approach to cybersecurity of the digital commons.

Our proposed framework is based on a community-centered, systems-thinking approach with a bottom-up methodology to change the current state of cyber-aloofness. This bottom-up approach is fueled by the concept of resilient communities and is based on the three foundational principles of innovative learning, awareness and adaptability, as pointed out earlier and as outlined in Fig. 2.

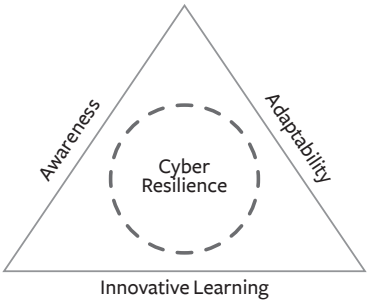


Fig. 2. A framework for cyber resilience.

Innovative Learning

The realization that digital grids around the world are a "commonly shared resource" would shift the task of cybersecurity from being someone else's responsibility to each and every individual user. Prior research has touted the power of change that is created "within" at the community level, where social, economic, cultural, and historic backgrounds are contextualized in the response to adverse events.[47,48] Leveraging innovative learning to create and sustain resilient communities is based on the premise that governments and institutional bodies are not the sole drivers of cyber resilience, although they can be an instrumental coordinator and sponsor. Therefore, a community-level focus on resilience promotes local engagement, accountability and flexibility in building cyber resilience.

In addition, a bottom-up approach would typically integrate social and structural aspects of cybersecurity, which are often overlooked, to drive change and investigate the root cause of cybersecurity risks at a deeper level. Further, a bottom-up community-based approach enables groups to acquire relevant institutional memory.[49,50] This localized knowledge can be leveraged by communities around the world, in accordance with their unique modes of learning and social attributes, to create a runaway process and momentum towards a tipping point in cyber resilience. Additionally, strengthening the capacity of community resilience can help build cyber resilience at the national or international levels, instead of fostering institutional or governmental dependencies.

Awareness

Despite the availability of sophisticated digital controls, technological countermeasures alone remain insufficient to protect users from online threats. Cyber controls can be rendered ineffective by the click of a button. The end-users are responsible for embracing privacy controls, using complex passwords, and adhering to cybersecurity policies and best

practices. A widely known cliché in cybersecurity is that "humans are the weakest link."[51] Lately, this cliché has met some pushback, with articles suggesting that humans are doing the best they can in the complex networked environments that they inhabit. Proponents of both these lines of contradicting thought agree that awareness is a key part of defense in the war against cybercrime.

In cybersecurity, the concept of awareness tends to manifest itself in the form of awareness programs and campaigns designed to educate and inform users to reduce risks.[52] While awareness programs can help develop resilience through the acquisition of knowledge needed to anticipate and respond to events, there are limitations to current approaches. Prior scholars noted that the predominantly used rule-based cybersecurity awareness training methodologies may not be effective in fending off attacks in the long run.

Cybersecurity awareness, as it exists today, largely remains a "check-the-box" compliance exercise and does not promote and sustain a deeper sense of mindfulness to achieve higher levels of resilience. Recent research has outlined three primary limitations of traditional rule-based cybersecurity awareness efforts: a superficial sense of mastery, lack of sufficient defenses against new and complex attacks, and inadequate ability to cultivate cognitive faculties to defend against sophisticated attacks. Furthermore, researchers have noted that there are differences in the mental models of security experts and non-expert users, which may result in communication and training gaps for mitigating cybersecurity risks.[53]

We argue that cybersecurity mindfulness extends beyond the scope of an individual. It is a broader and deeper sense of traditional cybersecurity awareness, and can be leveraged as an important building block to develop a "human firewall" culture within resilient communities. The ability to leverage the practice of cybersecurity mindfulness to make conscious and informed decisions can mean the difference between success and failure in cyber space. However, mindfulness as a building block of resilience is limited if it does not extend beyond the scope of an individual: resilient communities are built on interconnected structures of innovative learning, awareness, and adaptability.

Adaptability

Cyber security threats continue to evolve at a staggering pace and scale affecting all kinds of online entities. The policies, procedures, and controls that are developed in response to a particular threat must be continuously revised to counter different kinds of attacks and threats in different domains. Adaptability is, therefore, a key component of cyber resilience, where the solution frameworks are most effective if they are tailored to organizations and their capabilities. One resource for studying adaptability in cyber resilience can be found in the field of complex adaptive systems (CAS). Prior scholars have demonstrated that CASs such as networks, behavior is instigated by the collective and parallel actions of agents within a system, and not by a single entity.[54] Likewise, in cyber resilience, individuals and

institutions need to be equipped to respond to their changing environments, to create mental models for interpretation and analysis of threats, and to work together to adapt and thus increase the resilience of their networks and systems.

COMMUNITY-CENTRIC APPROACHES TO CYBER RESILIENCE

A lot has been written about the opacity of cybersecurity information sharing. Attacks are often not reported either by individuals or organizations. Often, the reports of these incidents are intentionally vague or opaque about the attack vector.[55,56] While certain information is deemed unallowable to share based on national security or governance interests, other cybersecurity-related information that can be shared widely stands to benefit cyber resilience strategies in cross-sector and in-sector organizations.[57-59] Additional approaches for promoting cyber resilience through responsible use of the cyber commons involve composable governance[60] and equifinality.[61] Composable governance refers to customizable frameworks of governance for specific domains of application, whereas equifinality offers stakeholders the ability to adopt solution bundles that fit their needs for ensuring cyber resilience. Table 1 provides a summary of various mechanisms discussed in this paper for achieving cyber resilience. These mechanisms are broadly classified into three categories: technical, governance, and social. It must be noted that these categories are not exclusive: overlap among categories and the encompassing mechanisms is key to enabling stakeholders in achieving cyber resilience.

Community-centric mechanism for cyber resilience	Description
Technical	- Support encryption - Share vulnerabilities, threat information, and countermeasures - Enterprise risk management
Governance	- Local governance of digital commons - Composable governance60 - Equifinality
Social	- Holistic cybersecurity - Social learning - Cultivating a culture of cybersecurity (cybersecurity mindfulness, human firewalls, communities of trust)

Table 1. Community-centric approaches to cyber resilience

One example of information sharing for achieving cyber resilience is in the Common Vulnerabilities and Exposures (CVE) dictionary.[62] Developed with support from The MITRE Corporation and the United States Department of Homeland Security (DHS), the Common Vulnerabilities and Exposures (CVE) dictionary has come to exemplify a community-led effort to share information about flaws, their severity, their scope, and associated countermeasures. Prior to the development of the CVE dictionary, vulnerabilities were classified, scored, and identified differently depending on the vendor, leading to impeded interoperability and information-sharing. The success of the CVE has spurred several derivative initiatives, such as MITRE's Common Weakness Enumeration (CWE) dictionary of software weaknesses[63] and the CVE Change Logs tool[64] to track changes to the CVE list. Widespread support for the CVE has facilitated its de facto status, where cybersecurity vendors make their products

compatible with the CVE dictionary identifiers. Other examples of community initiatives in cybersecurity that are already showing promise are National Science Foundation's (NSF) Cybersecurity Center of Excellence called Trusted CI,[65] Cybersecurity and Infrastructure Security Agency's (CISA) Connected Communities Initiative,[66] and its Joint Cyber Defense Collaborative (JCDC),[67] which are some of several public-private partnerships being developed for capacity-building efforts against cybercrime.

One particular success story is the 2021 Tokyo Olympic and Paralympic Games.[68] The organizers of the Tokyo Olympics incorporated cybersecurity in the Olympic infrastructure from the start, and utilized an international team of cybersecurity experts. Nippon Telegraph and Telephone (NTT) corporation, which was responsible for providing the network and communications support for the Tokyo Olympics, reported they had thwarted 450M cybersecurity attacks targeted toward the Tokyo Olympics. Training and awareness campaigns for staff prior to the Olympics, advanced communication networks, and specialized cybersecurity infrastructure including personnel support helped the organizer of the 2021 Olympic Games secure the physical and digital infrastructure from an unprecedented number of attacks (the number of attacks was reported to be 2.5 times that of the London Olympics).

DISCUSSION

The discussion in this paper so far has centered on the idea that cybersecurity, woven along with innovative learning, awareness, and adaptability, contributes to the theory and practice of cyber resilience. The community-centered cyber resilience framework proposed in this paper has several implications for cyber security; we highlight a few key implications below.

The Role of Agency

User perceptions and mental models of cybersecurity best practices vary, and this variance impacts the agency of individuals and organizations in creating cyber resilience. Here, agency refers to the abilities of end users regarding both the acquisition of information about cybersecurity best practices as well as their implementation. The acquisition of such information is challenging due to various factors: lack of requisite technical skills, conflicting guidance, lack of clear policies, and an inability to discern the appropriate information pertaining to specific threat scenarios. In contrast to learning or acquiring information from experience (or empirical learning), which is often fraught with challenges, learning from social observation is far more effective. Information about a cyberattack can provide valuable lead time and learning opportunities for others who can avoid becoming the next victim of the attack. Social learning offers agency to each individual and organization in their efforts to secure their digital networks and is critical to developing a culture of cybersecurity that eventually fosters innovations. In fact, social learning that relies heavily on cognitive innovations has been observed as a critical component of cultural transmission in both human and animal societies.[69, 70]

Agency also confers upon agents the valuable attribute of adaptability. Faced with complex environments like the digital commons, individuals and communities have shown that they are predisposed with a willingness to interpret and implement guidelines in ways that make the most sense for their own values.[71] Adaptability, therefore, is key to dealing with the dynamic nature of the digital commons. Conflicting guidance and implementation in cybersecurity was found to be a consequence of value conflicts, where varying values of stakeholders in the digital commons included fairness, economic costs, and prevention of harm to information and physical assets.[72] Further, individual traits and responses to secure behavior in the digital commons differ.[73,74] These examples suggest that countermeasures to address the ToC problem in cybersecurity should consider the role of agency in a community-centered approach. Such an approach relieves individuals and communities of the burden of coming up with global solutions, and addresses the "awareness" aspect of our proposed framework. Instead, local solutions to secure networks can be adopted as the first step to securing regional and then larger, global networks for promoting cyber resilience.

Beyond Regulation

The idea of cultivating resilient communities to reach a tipping point in cybersecurity aligns with Ostrom's solution framework, which calls for mechanisms beyond regulation to combat the ToC problem. While leveraging innovative learning to build resilient communities may take several forms, prior research[75] outlines four factors that can be considered for building resilience. These include the ability to embrace change and uncertainty, fostering diversity to reduce risks, optimizing knowledge and problem-solving abilities, and creating opportunities for self-organization while reinforcing the role of local engagement, thus addressing the "adaptability" component of our proposed framework for a community-centered approach to cyber resilience.

Resilience Assurances

Good cybersecurity practices, first and foremost, provide an assurance of stability. This assurance has value not just when the cybersecurity countermeasures work as intended, but also when they fail and attackers have the upper hand. In the latter case, especially, the assurance of stability carries a greater value since it offers the attribute of resilience to the networks. Modern-day networks are engineered for confidentiality, integrity, and availability (CIA), and threat vectors are constantly seeking to disrupt one or more of these assurances. Incorporating cyber resilience as an additional assurance will have significant impact on the ability of networks to withstand attacks to CIA. However, such an approach for incorporating cyber resilience will only be effective if it is designed with a focus on communities. Communities and networks share many structural traits, and the impact of cyber resilience can be most effective when leveraged with a focus on communities and social cohesiveness.

CONCLUSION

Despite billions of dollars spent each year on cyber-defense initiatives, global cybersecurity cooperation continues to lag, without consolidating efforts to empower users and communities around the world. In this article, we analyzed the role that communities can play in improving the resilience of our online environments through the perspective of the tragedy of cyber commons. Unlike the tragedy of environmental commons where a single finite resource is driven to extinction, the cyber commons that we inhabit comprise of resources required to create, maintain, and sustain these commons. This paper presented a bottom-up approach supported by resilient communities that would be critical to fuel change from within our communities to combat the global problem of tragedy of the cyber commons. Getting past the tragedy of commons in cybersecurity requires a certain level of collective resilience to sustain our shared digital environments. The proposed framework in this paper is intended to serve as a blueprint for cultivating and promoting community-centered cyber resilience, while strengthening global cyber defense capabilities in the process.

NOTES

1. Garrett Hardin, "The tragedy of the commons," *Science* 162, no. 3859 (Dec. 1968) https://doi.org/10.1126/science.162.3859.1243.
2. Lawrence Lessig, "Code and the Commons," *Conference on Media Convergence*, Fordham Law School, New York, NY (1999).
3. William Lehr and Jon Crowcroft, "Managing shared access to a spectrum commons," in *Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks* (2005), available at https://doi.org/10.1109/dyspan.2005.1542658.
4. Mélanie Dulong de Rosnay and Felix Stalder, "Digital commons," *Internet Policy Review,* Alexander von Humboldt Institute for Internet and Society 9, no. 4 (2020), https://doi.org/10.14763/2020.4.1530.
5. Daniel McFadden, "The tragedy of the commons," *Forbes*, https://www.forbes.com/asap/2001/0910/061_2.html.
6. Nicolas Curien, Emmanuelle Fauchart, Gilnert, G., and Franceau Moreau, "Online consumer communities: Escaping the tragedy of the digital commons, *Internet and Digital Economics* (2007) https://doi.org/10.1017/cbo9780511493201.006.
7. Eytan Adar and Bernardo Huberman, "Free riding on Gnutella," *First Monday* 5, no. 10 (2000), https://doi.org/10.5210/fm.v5i10.792.
8. Seva Gunitsky, "Corrupting the cyber-commons: Social media as a tool of autocratic stability," *Perspectives on Politics* 13, no. 1 (2005), https://doi.org/10.1017/s1537592714003120.
9. Charles Schweik, "Sustainability in open source software commons: lessons learned from an empirical study of Sourceforge projects," *Technology Innovation Management Review* 3, no. 1 (2013), https://doi.org/10.22215/timreview/645.
10. Gian Maria Greco and Luciano Floridi, "The tragedy of the digital commons," *Ethics and Information Technology* 6, no. 2 (2004), https://doi.org/10.1007/s10676-004-2895-2
11. Virgilio Almeida, Fernando Filgueiras, and Francisco Gaetani, "Digital governance and the tragedy of the commons," *IEEE Internet Computing* 24, no. 4 (2020), https://doi.org/10.1109/mic.2020.2979639.
12. Roger Hurwitz, "Depleted trust in the cyber commons," *Strategic Studies Quarterly* 6, no. 3, 20-45 (2012).
13. Mark Raymond, "Puncturing the myth of the Internet as a commons," *Georgetown Journal of International Affairs* (2005), available at https://www.jstor.org/stable/43134322.
14. Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons," In *Law and Society Approaches to Cyberspace*, Routledge (2005), https://doi.org/10.4324/9781351154161-3
15. Patricia Longstaff, Nicholas Armstrong, Keli Perrin, Whitney Parker, and Matthew Hidek, "Building resilient communities: A preliminary framework for assessment," *Homeland Security Affairs* 6, no. 3 (2010), https://securitypolicylaw.syr.edu/wp-content/uploads/2012/09/Building-Resilient-Communities.pdf.
16. Elinor Ostrom, "Tragedy of the comons,: in The New Palgrave Dictionary of Economics, S.N. Durlauf and L.E. Blune, Eds, 2nd ed. Palgrave Macmillan (2008), https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/5887/tragedy%20of%20the%20commons%20_%20Th...pdf.
17. Donella H. Meadows, T*hinking in systems: A primer,* D.Wright, Ed., White River Junction, Vermont, USA: Chelsea Green Publishing (2008).
18. Jaye Wald, Steven Taylor, Gordon Asmundson, Kerry Jang, and Jennifer Stapleton, "Literature review of concepts," *Psychological Resiliency* 134, (2006).
19. Helen Herrman, Donna E. Stewart, Natalia Diaz-Granados, Elena L. Berger, Beth Jackson, and Tracy Yuen, "What is resilience?," Canadian Journal Of Psychiatry. *Revue canadienne de psychiatrie* 56, no. 5, (2011), https://doi.org/10.1177/070674371105600504.
20. Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, "Developing cyber-resilient systems: A systems security engineering approach," *NIST SP 800-160* vol. 2 (2021), available at https://doi.org/10.6028/NIST.SP.800-160v2r1.
21. Omera Khan, Daniel A.S. Estay, "Supply chain cyber-resilience: Creating an agenda for future research," *Technology Innovation Management Review* 5, no. 4 (2015), http://doi.org/10.22215/timreview/885.
22. Adrian Davis, "Building cyber-resilience into supply chains," *Technology Innovation Management Review* 5, no. 4 (2015), http://doi.org/10.22215/timreview/887.

NOTES

23. Luca Urciuoli, "Cyber-resilience: a strategic approach for supply chain management," *Technology Innovation Management Review* 5, no. 4 (2015), available at https://doi.org//10.22215/timreview/886
24. Mohammad Ghiasi, Moslem Dehghani, Taher Niknam, and Abdollah Kavousi-Fard, "Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power systems," *Network* 1, no. 1 (2020), https://www.academia.edu/42209946/Investigating_Overall_Structure_of_Cyber_Attacks_on_Smart_Grid_Control_Systems_to_Improve_Cyber_Resilience_in_Power_System.
25. Andrea Salvi, Paolo Spagnoletti, and Nadia S. Noori, "Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem," *Computers & Security* 112 , no. 102507 (2022), https://doi.org/10.1016/j.cose.2021.102507.
26. Andrew D. Syrmakesis, Cristina Alcaraz, and Nikos D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *International Journal of Information Security* 21 (2022), https://doi.org/10.1007/s10207-022-00594-7.
27. Mariana Segovia, Jose Rubio-Hernan, Ana R. Cavalli, and Joaquin Garcia-Alfaro, "Cyber-resilience evaluation of cyber-physical systems," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)* (2020), https://doi.org//10.1109/NCA51143.2020.9306741.
28. Md. Ariful Haque, Gael K. De Teyou, Sachin Shetty, and Bheshaj Krishnappa, "Cyber resilience framework for industrial control systems: concepts, metrics, and insights," in *Proceedings of the IEEE International Conference on Intelligence and Security Informatics* (ISI) (2018), https://doi.org//10.1109/ISI.2018.8587398.
29. Kathleen Tierney, and Michel Bruneau, "Conceptualizing and measuring resilience: A key to disaster loss reduction," *TR News*, no. 250 (2007), https://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf
30. Benoit Dupont, "The cyber-resilience of financial institutions: significance and applicability," *Journal of Cybersecurity* 5, no. 1 (2019), https://doi.org/10.1093/cybsec/tyz013.
31. Deborah Bodeau, Richard D. Graubart, Rosalie M. McQuaid, and John Woodill, "Cyber resiliency metrics, measures of effectiveness, and scoring," *MITRE Corp* (2018), https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.
32. NIST, "Framework for improving critical infrastructure cybersecurity version 1.1: NIST Cybersecurity Framework," *NIST* (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
33. ISO, "Risk Management – Guidelines," *ISO 3100,* Geneva, Switzerland, 2018.
34. Abraham Althonayan and Alina Andronache, "Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment," in *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (2019), https://doi.org/10.1109/CyberSA.2019.8899445.
35. Samir Jarjoui and Renita Murimi, "A framework for enterprise cybersecurity risk management," in *Advances in Cybersecurity Management*, K. Daimi and C. Peoples, eds., Cham, Switzerland: Springer (2021), 139–161, https://doi.org/10.1007/978-3-030-71381-2_8.
36. Robert Ramirez and Nazli Choucri, "Improving interdisciplinary communication with standardised cyber security terminology: a literature review," *IEEE Access*, vol. 4, 2016, 2216–2243, https://doi.org/10.1109/ACCESS.2016.2544381.
37. Samir Jarjoui, Robert K. Murimi, and Renita Murimi, "Hold My Beer: A case study of how ransomware affected an Australian beverage company," in *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, IEEE Xplore (2021), https://doi.org/10.1109/CyberSA52016.2021.9478239.
38. Cisco, "Achieving security resilience," Security Outcomes Report, vol. 3, 2022, https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html.
39. Hans D. Bruijn and Marijn Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Gov. Inf. Q.* (34), no.1 (2017), https://doi.org/10.1016/j.giq.2017.02.007.
40. Van Nes, Egbert H., Babak MS Arani, Arie Staal, Bregje van der Bolt, Bernardo M. Flores, Sebastian Bathiany, and Marten Scheffer, "What do you mean,'tipping point'?." *Trends in Ecology & Evolution* 31, no. 12 (2016), https://doi.org/10.1016/j.tree.2016.09.011.
41. Malcolm Gladwell, "*The Tipping Point: How Little Things Can Make a Big Difference*," New York: Little, Brown and Company (2000).

NOTES

42. Mahdi Roghanizad, Ellen Choi, Atefeh Mashatan, and Ozgur Turetken, "Mindfulness and cybersecurity behavior: A comparative analysis of rational and intuitive cybersecurity decisions," *AMCIS 2021 Proceedings* 13 (2021), available at https://aisel.aisnet.org/amcis2021/info_security/info_security/13
43. Leah Zhang-Kennedy and Sonia Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Computing Surveys* (CSUR) 54, no. 12 (2022), https://doi.org/10.1145/3427920.
44. Ben Buchanan, *The cybersecurity dilemma: Hacking, trust, and fear between nations*, Oxford University Press, 2016.
45. Glyn Moody, "Dutch government: encryption good, backdoors bad", Ars Technica, 6 January 2016.
46. Japan NISC, "Outline of the Cybersecurity Strategy" (2021), https://www.nisc.go.jp/eng/index.html.
47. Fran H. Norris, Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness," *American Journal of Community Psychology* 41, no. 1-2 (2008), https://doi.org/10.1007/s10464-007-9156-6.
48. Marcus Collier, Zorica Nedović-Budić, Jeroen C. Aerts, Stuart Connop, Dermot Foley, Karen M. Foley, Darryl J. Newport, Siobhan Mcquaid, Alexander Slaev, and Peter H. Verburg, "Transitioning to resilience and sustainability in urban communities." *Cities* 32 (2013), https://doi.org//10.1016/J.CITIES.2013.03.010.
49. Cem Sen, Korhan Arun, and Olkay Okun, "Organizational memory: A qualitative research on a multi-cultural organization," *Kybernetes* (2021), https://doi.org/10.1108/K-08-2021-0783.
50. Robert L. Cross and Andrew Parker, *The Hidden Power Of Social Networks: Understanding How Work Really Gets Done In Organizations*, Harvard Business School Press, Boston (2004), https://www.bu.ac.th/knowledgecenter/epaper/jan_june2010/pdf/Page_155.pdf
51. Martina A. Sasse, Sacha Brostoff, and Dirk Weirich, "Transforming the 'Weakest Link'—a human/computer interaction approach to usable and effective security," *BT Technical Journal* 19 (2001), https://doi.org/10.1023/A:1011902718709.
52. Matthew L. Jensen, Michael Dinger, Ryan T. Wright, and Jason B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *Journal of Management Information Systems* 34, no. 2 (2017), https://doi.org/10.1080/07421222.2017.1334499.
53. Robert Murimi, Sandra Blanke, and Renita Murimi, "A decade of development of mental models in cybersecurity and lessons for the future," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science* (2022), https://doi.org/10.1007/978-981-19-6414-5_7.
54. Kevin J. Dooley, "A complex adaptive systems model of organization change," *Nonlinear Dynamics, Psychology, and Life Sciences* 1, no. 1 (1997), https://doi.org/10.1023/A:1022375910940.
55. Waleed Alkalabi, Leonie Simpson, and Hasmukh Morarji, "Barriers and incentives to cybersecurity threat information sharing in developing countries: a case study of Saudi Arabia," in *Proceedings of the Australasian Computer Science Week Multiconference* (2021), https://doi.org/10.1145/3437378.3437391.
56. Priscilla Koepke, "Cybersecurity information sharing incentives and barriers," in *Proceedings of the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity*, MIT Sloan School of Management (2017), https://cams.mit.edu/wp-content/uploads/2017-13.pdf.
57. David Turetsky, Brian Nussbaum, Unal Tatar, "Success stories in cybersecurity information sharing," in Proceedings of the SUNY Albany Cybersecurity Conference (2018), https://www.albany.edu/sscis.
58. Derek Manky, "The hard truth and good news about the fight against cybercrime," Forbes (2021), https://www.forbes.com/sites/fortinet/2021/05/17/the-hard-truth-and-good-news-about-the-fight-against-cybercrime/?sh=3adc2dce19b5.
59. Michael Daniel, "How global information sharing can help stop cybercrime," *Harvard Business Review* (2023), https://hbr.org/2023/06/how-global-information-sharing-can-help-stop-cybercrime.
60. Renita Murimi, "Governance in DAOs: Lessons in Composability from Primate Societies and Modular Software," *MIT Computational Law Report* (2022), available at https://law.mit.edu/pub/governanceindaos
61. Brett J. L. Landry, Renita Murimi, and Greg Bell, "Building equifinality and improvisation into effective cyber operations,". In *Effective Cybersecurity Operations for Enterprise-Wide Systems,* F. Adedoyin and B. Christiansen (Eds.) IGI Global (2023), https://doi.org/10.4018/978-1-6684-9018-1.ch009.
62. Common Vulnerabilities and Exposures, https://cve.mitre.org/.
63. Common Weakness Enumeration (CWE), https://cwe.mitre.org/.

NOTES

64. History of the CVE, https://www.cve.org/About/History.
65. NSF Trusted CI,. https://www.trustedci.org/.
66. CISA Connected Communities, https://www.cisa.gov/topics/risk-management/connected-communities.
67. CISA Joint Cyber Defense Collaborative (JCDC), https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.
68. Brian Gant, "The Tokyo Olympics are a cybersecurity success story," *Security Magazine* (2021), https://www.security-magazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story.
69. Robin Dunbar, "*Grooming, Gossip, and the Evolution of Language,*" Harvard University Press (1996).
70. Amanda Seed and Michael Tomasello, "Primate cognition," *Topics in cognitive science* 2, no. 3, https://doi.org/10.1111/j.1756-8765.2010.01099.x
71. Ameya Hanamsagar, Simon Woo, Christopher Kanich, and Jelena Mirkovic, "How users choose and reuse passwords," *Information Sciences Institute* (2016).
72. Marcus Christen, Bert Gordijn, Karsten Weber, Ibo Van de Poel, and Emad Yaghmaei, "A review of value-conflicts in cybersecurity: an assessment based on quantitative and qualitative literature analysis," *The ORBIT Journal* 1, no. 1 (2017), https://doi.org/10.29297/orbit.v1i1.28.
73. Michael Fagan and Maifi Khan, "To follow or not to follow: a study of user motivations around cybersecurity advice," *IEEE Internet Computing* 22, no. 5 (2018), https://doi.org/10.1109/mic.2017.3301619.
74. Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther, "Correlating human traits and cyber security behavior intentions," *Computers and Security* 73 (2018), https://doi.org/10.1016/j.cose.2017.11.015.
75. Fikret Berkes, "Understanding uncertainty and reducing vulnerability: lessons from resilience thinking," *Nat Hazards* 41 (2007) available at https://doi.org/10.1007/s11069-006-9036-7.