EPiC Series in Computing

Volume 63, 2019, Pages 90–100

Proceedings of 32nd International Conference on Computer Applications in Industry and Engineering

A Purposeful Systems Design Approach for Cybersecurity

Maximilian M. Etschmaier
Florida State University
metschmaier@fsu.edu

Abstract

The paradigm of purposeful systems is used to analyze and define cyberspace as a collection of functions that are to be provided and preserved if harm to various elements of the space is to be avoided. We consider harm to individuals, groups of humans, as well as humanity as a whole and identify an overall systems approach to regulating cyberspace that can guide efforts currently undertaken by various governmental and industry organizations. The approach is based on clear universal ethical principles. The result will harness the full potential of cyberspace while eliminating opportunities for "bad actors" to reap undue benefits at the expense of individuals and the community.

1 Introduction

What today is commonly referred to as cyberspace grew from an effort to develop a robust computer-based system of many-to-many communication that could survive a hostile environment such as a military conflict. Different from the telegraph and telephone systems that required the existence of a communication channel between the endpoints of the communication for the duration of the communication, the communication was broken up into discrete packets, each of which could independently find its way through a network of communication links. Thus, a communication will not break down when individual links fail or are congested. The price for this is an increase in the complexity of the communication. Instead of just inert data, it also needs to include parts of code that, combined with code and data that reside elsewhere, will dispatch a packet toward its destination. The same mechanism can also be used to distribute the execution of programs among various processors. For example, the originator of a communication can include code in the message that the recipient can use to turn the message into usable information. And it may cause the code to be stored in the processor of the recipient for application to future messages. Additional complexity is introduced because ownership and control of the system may be divided between numerous entities which cannot be assumed to share the same motives and objectives.

In a short span of time, scope and functionality of this system evolved opportunistically to fundamentally change the way individuals, groups, and societies interact and business is conducted. In

Q. Yuan, Y. Shi, L. Miller, G. Lee, G. Hu and T. Goto (eds.), CAINE 2019 (EPiC Series in Computing, vol. 63), pp. 90–100

addition, as in any system, complexity brings about the possibility of errors in design, which in themselves may produce harmful results, and beyond that, may be exploited to the detriment of the operators and users of the system.

Restraining and mitigating negative outcomes is proving to be increasingly difficult and laden with conflicts between various principles and expectations. In general terms, this is the aim of what is commonly called cybersecurity. However, there are wide differences in what is considered the scope [1]. And it is those differences that explain the differences in approaches, methods, objectives, and rights and responsibilities of the various participants in any segment of cyberspace. We are proposing a rational, holistic framework through which it should be possible to analyze and interpret any existing or proposed approach or measure intended to achieve security for all or parts of cyberspace. The framework is based on the paradigm of purposeful systems which we have introduced [2].

In this paper, we will review some examples of threats that have arisen in cyberspace to show the wide variety of forms that threats can take on and examine mitigation measures that have been developed or proposed. Then we will present selected features of cyberspace within the framework of the purposeful systems paradigm. We will show that, while there are specific technical constructs that can provide threat mitigation in some situations, there are other situations where mitigation is dependent on proper assignment of responsibilities to the different players in cyberspace or on a particular formulation or interpretation of legal and constitutional provisions, as well as ethical norms. We will show that the greatest threat from cyberspace arises from the interdependence of its evolution with that of humanity and the human sphere. Finally, we will show that cybersecurity is not attainable as long as there are powerful interests that derive enormous benefit from its absence.

2 Defining Cybersecurity

The annual report of the Internet Crime Complaint Center ("ic3") of the FBI lists 34 different types for the 351,937 cybercrime complaints in 2018, the vast majority of which involved some form of financial loss by the victim [3]. Other types of cybercrime include the theft of information by gaining unauthorized access to computers and planting "malware" on the victim's computer. Interestingly, these types appear to break down a crime into its components, which might obscure the whole extent of a crime and focus mitigation efforts on technological issues. For example, extortion through "ransomware" is divided into several separate acts, including the development and publication of software, the transmission of the software to the computer systems of the victim, and the facilitation of clandestine payment of the ransom through cryptocurrency [4]. It is not surprising then that ic3 would feel relatively powerless and recommend that vulnerable institutions focus on "contingency and remediation planning [as] crucial to business recovery and continuity" [5]. It appears that the FBI is limiting its view of cybercrime to the actual infliction of harm, and its role to solving and prosecuting a crime after it has occurred and that it places the onus for prevention on the victim.

This interpretation appears to be echoed by the definition of cybersecurity offered by Craigen et al. as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" [6]. However, if, as argued in their paper, property rights are understood as a multidimensional concept of public good within the commons as advocated by Ostrom [7], the definition may well serve as one point of departure for the development of holistic constructs of security in cyberspace.

Expanding on the characterization of cybersecurity as a public good, Mulligan and Schneider point to parallels with public health in public policy, law and enforcement, where the interests of individuals and the public do not always align, and laws and frameworks can mediate tensions between them[8]. "Success ultimately depends not only on technical progress but on reaching a political agreement about

(i) the relative value of a public good in comparison to other societal values and (ii) the institutions granted authority to resolve conflicts (and the methods they use)."

3 Achieving Cybersecurity

There is widespread agreement that it is not possible to achieve cybersecurity through technical means alone, but that a holistic approach is necessary to develop a viable framework and processes that can mediate between the sometimes-conflicting expectations of the various players in cyberspace. However, many frameworks restrict themselves to tangible effects that can be quantified and ultimately reduced to the common denominator of money. Benefit-cost analysis – or its probabilistic equivalent, risk analysis – is then used as a basis for decision-making. This is the problem. Even when the quantification is only conceptual, it permits the illusion of rationality and optimality of an approach and a solution, while ignoring the intangible dimension. But it is the intangible dimension, which includes ethical considerations, that is critical to the success of a system that involves humans and machines and especially one that spans the whole of the human sphere, as cyberspace increasingly does.

It is widely recognized that tools of cyberspace can influence the opinion and choices of individuals and groups. This is what all forms of communication have always been used for. The powers unleashed by cyberspace are just unfathomably more powerful and differentiated. It has already been proven that it can sway the outcome of democratic elections toward otherwise unlikely candidates and causes, potentially choosing between war and peace or life and death for millions [9]. With its global spread, cyberspace can alter the direction of evolution of the human sphere and impact the sustainability of humanity and the conditions for human survival. This may open exciting new possibilities. It also opens the possibility of humans losing control of their own destiny [10]. The choice of an approach for achieving cybersecurity thus is a moral choice that is critical to the future of humanity.

"There are few areas where this is more important than privacy," remarked Apple CEO Tim Cook at the Stanford University commencement on June 16, 2019. "If we accept as normal and unavoidable that everything in our lives can be aggregated, sold, or even leaked in the event of a hack, then we lose so much more than data. We lose the freedom to be human. Think about what's at stake. Everything you write, everything you say, every topic of curiosity, every stray thought, every impulsive purchase, every moment of frustration or weakness, every gripe or complaint, every secret shared in confidence." [11]

Part of any effort to achieve cybersecurity is to question prevailing views and examine to what extent they have been shaped by powerful players in cyberspace to their benefit. For example, Schwartz takes issue with efforts to tackle "deepfakes," purposely false information, through technological means, proclaiming that "deepfakes aren't a tech problem. They're a power problem" [12]. The search for technological solutions to all problems related to cyberspace may divert attention from the real causes of these problems, the business models of the tech industry and the perceived needs of national security organizations and military services. In addition, it may create business opportunities for the tech industry and research institutions and ultimately make society more and more dependent on their solutions.

We believe that the paradigm of purposeful systems can provide a framework for re-examining the evolution of cyberspace and for developing a new model for cybersecurity. Our past work examining systems ranging from simple technological systems to global environmental sustainability gives us confidence that the purposeful system paradigm does provide a suitable framework and will yield results that are consistent with, and can add to, a model of global sustainability. In the following, we briefly outline the central features of the paradigm of purposeful systems as they pertain to the present problem and show how a sustainable solution can be developed.

4 The Purposeful Systems Approach

The paradigm of purposeful systems views any system as a construct, the boundary of which is drawn in such a way that the system purpose, to the extent possible, is included within it. Designing a purposeful system is an iterative process of defining and redefining the scope (or boundaries) and purpose until this balance is achieved. The mechanism of iteration between purpose and scope continues throughout the entire life of the system, driven by a "historian" who develops insight into the nature and behavior of the system, and a "designer" who turns the insight into modifications of functions and scope of the system. This requires the participation in the system of a being that is capable of insight and reasoning, like a human element. The result is a system that, similar to a living organism, can learn and adapt to a changing environment posing emerging threats to its existence. The system possesses consciousness of itself and its environment. An essential part of the system purpose is avoidance of "critical failures" from which there is no recovery. The design process eliminates the possibility of critical failures through proper design of system functions. The only exceptions are potential failures, the possibility of which cannot be recognized within the state of the art. In such cases, the resilience that results from the self-consciousness of the purposeful system will provide mitigation. Examples from our past work for the design of a purposeful system range from relatively simple technological systems [13-14] to a design for achieving global environmental sustainability [15].

5 Ontology of Cyberspace and Cybersecurity

Cyberspace is an extremely complex system that is affecting much of human existence in many ways. Since it has evolved in an opportunistic manner and without much central coordination, its structure and the interaction between its various components as well as the interdependence between its functions are not easily recognized in all their complexities.

Figure 1 shows a top-level view of cyberspace and can serve as a point of departure for analysis as a purposeful system. The figure is divided into four sections:

i. The "physical" network infrastructure that handles all transmission and routing of communication among users and between users and various communication platforms like social media and filesharing, user services like search engines, and shopping and financial transaction services. The network infrastructure also provides direct links to entities in section iii.

ii. The individual users, service providers, and platforms and user services. These, together with the network infrastructure, represent the original view of cyberspace as perceived by individual and business users. For a fee, users connect to a service provider who manages their communication across cyberspace and defines their user experience.

iii. Commercial entities that may extract data for use toward a variety of purposes, including predicting and influencing personal tastes and shopping behavior, as well as political preferences; and various governmental agencies especially concerned with national security and defense that monitor traffic in order to identify emerging threats to national security and a variety of illegal activities. All these entities, in addition to using the network infrastructure for their own communications, draw significant benefits from their access to user communications and in return often provide free services to the users. This is their ultimate value proposition.

iv. The highest section concerns the impact that activities in cyberspace may have on national and global economic, social, political and natural systems. This may be perceived as largely unintentional. Decision-makers may view it as coincidental externalities. However, it is becoming increasingly clear that forces emerging through cyberspace can literally change the course of human evolution. This may well be recognized by certain interest groups as an opportunity to shape the future of the human sphere according to their vision.

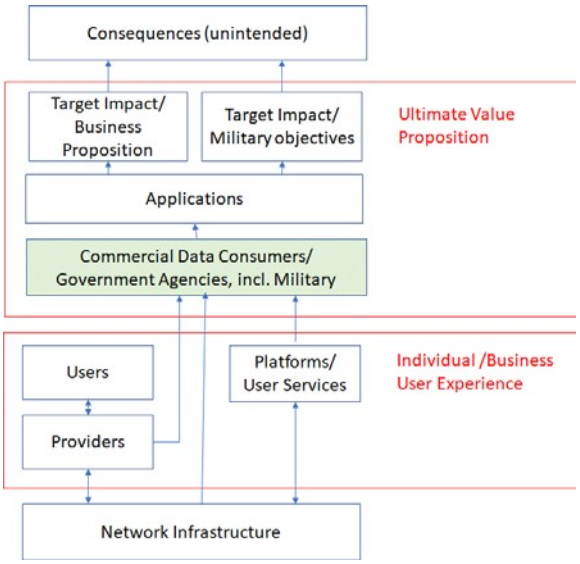

Figure 1: Overview of the components of cyberspace and their interactions

6 Analysis of Potential Harm

The system "Cyberspace" is made up of countless functions and components, each of which may be impacted by various types of threats. The purpose of the design of this system must be to assure the availability of functions when needed. The focus must be on "critical functions," the loss of which would be an irreversible "critical failure." A system for which this cannot be assured is not fit for its intended purpose.

Threats may be the result of conscious action, possibly malicious, or they may arise unintentionally, for example, through faulty hardware, software, or data. They may originate from either within or outside the subject domain within cyberspace.

Functions can be grouped according to the system components they are attached to and which bear the ultimate harm. There are two such distinct categories of components that can be identified. Each one is subject to a unique set of threats which require specific functionalities within cyberspace to be mitigated so that they can be kept from leading to critical failures. The first category covers direct users, which include individual users like persons and businesses users, and groups of users comprising affinity groups, formal organizations, sovereign states, and the global human sphere.

Opposite to this category are components that have a stake in the mechanisms of cyberspace and are in a position to actively shape the structure of cyberspace and guide its evolution. Any measure to regulate cyberspace in order to avoid critical failures will target members of this category and limit their freedom. This category includes internet access providers; network platforms and user services; data consumers, commercial users and processors and resellers of data; government agencies; and national security and military organizations.

In the following, we shall focus on the first category of components and examine the types of critical failures they need to be protected against. Clearly, components of the second category are also exposed to potential critical failures. However, their failures are mostly of a technical nature and are the focus of much of the research in computer science and related disciplines. While they can trigger failures in

the first group of components, they are subsidiary to the overall system and receive their purpose from the first group. Their analysis, therefore, will have to follow the analysis of the first group.

6.1. Threats to Individual Persons

The concept that a person suffering irreparable harm constitutes a critical failure is not a new concept. At the very least, it evolved in civil aviation in the 1960s when it was recognized that an aircraft for which it might not be possible to prevent a critical failure, i.e., harm to human life, through operational procedures and maintenance actions would not be fit for service [16]. While in that case, harm to human life was interpreted as physical harm (and death), humans can be harmed in non-physical ways as well, and that harm may be graver and more persistent than physical harm. An extreme example of this is posttraumatic stress disorder of soldiers returning from combat. While non-physical harm may not kill a person outright, it may alter the essence of a human existence and ultimately deprive humans of their free will. Failures of cyberspace through threats to humans can take on many different forms, including threat to privacy, deprivation of access to reality and the truth, and threats to personal freedom and to property rights.

6.1.1. Threats to privacy

If we can view a human through the lens of a purposeful system, privacy is the space where introspection takes place. It is where the human examines input from the environment and uses it to adjust their sense of purpose and the reach of their person within the environment. Destruction of this space would deprive the person of their free will and turn them into a slave of the forces of their environment. In the ultimate state, any thought, any desire, and any affection would be intercepted by an external force and channeled into directions determined by that external force.

To some extent, limitation of privacy is a necessary part of any social system. It is the place where the commitment to a common ethical norm in a society resides, the glue that holds a community together. The threat to privacy from cyberspace is different. It is motivated by a quest for economic, social, and political power over other people. And it is wielded surreptitiously, piggy-backed on the need and desire of persons to communicate with friends, make new friends, and be part of a community; by their need to engage in commerce, to move around, and to operate everyday vehicles, machines and appliances. By providing a venue for communication, private companies like providers of internet access, operators of a social platform, or operators of any other internet-based service necessarily gain access to private information (data) transmitted through these communications. While much attention is being paid to protecting the information from access by “bad actors,” the service provider assures access to the information to themselves through clauses buried deep in the fine print of the user service agreement. For example, a recent study estimated that reading all the privacy notices an average user encounters in one year would take 76 eight-hour working days [17].

As cyberspace has significantly changed and grown into one of the most important business sectors and to be dominated by a small number of at least near-monopolistic players, there is no reason to continue the legislative and regulatory neglect. It may be time to consider prohibiting the use of information provided to cybernet service providers and to strictly limit access for government agencies. The model should be the extensive national legislation and regulation regarding the protection of privacy of the mail, as well as international treaties regulating trans-border communication which in one form or another have been in existence for centuries [18].

6.1.2. Deprivation of access to reality and the truth

From a technological perspective, cyberspace appears as a complex communication system through which information passes from some source to one or more destinations. During this passage, the information may be accumulated, aggregated, divided, sorted, and translated into a different format. Cybersecurity is a state of cyberspace that assures that the information is not materially changed by any of these processes without consent by the originating and receiving entities as it passes through cyberspace. Threats can arise from faulty design of the mechanisms of cyberspace, faulty intervention of human operators controlling the mechanisms, all unintentional; but also, from malicious intervention by hostile actors from outside of the space through which the information travels, or by rogue operators of the mechanisms within that space.

From a technical perspective, access to reality and truth is denied (a breach of cybersecurity) when information received at a destination is not consistent with information entered by any of the legitimate sources. Based on this definition, the information arriving at a destination may be considered "correct" or "incorrect." Determining correctness would require comparison of the information entered at the origin with the information arriving at the destination. This could be accomplished by using independent parallel channels or by comparing the value of a suitable statistic on the information at the origin and at the destination.

In situations when the information undergoes complex transformations between the origin and the destination, neither approach would work. In this case, some determination of the plausibility of correctness of the information arriving at the destination may be an alternative. Would such a measure of plausibility be robust enough to determine the effect of surreptitious, willful modification of the information? And, given knowledge of the measure of plausibility employed, would it be possible to construct modifications of the information that would evade detection? If this were possible, it would be necessary to find some other measure of truth or process of verification to determine if the message as received was correct.

Equally important, in an absolute sense, the question of reality and truth applies to the content of any message that enters cyberspace, i.e., before it undergoes any transformation within cyberspace. This includes how individuals or groups present themselves and their motives, as well as "artificial" humans ("bots") that are created to mislead. It also includes "Deep Fakes," fake photographic images created by AI algorithms.

There are efforts to determine the veracity of statements through algorithms of "Artificial Intelligence." Even if there were a chance for these to succeed, they would only increase the alienation of humans from the truth. Humans would lose confidence in their own judgment because they learn that their judgement is perceived as inferior to that of the algorithm. This diminishes the private space of individuals and with it the capacity for insight, another critical failure. Consequently, purely technological means do not appear suitable to protect against the threat to access to reality and the truth.

But there are other means to prevent critical failures. There is no reason a society should tolerate being bombarded by information they do not possess the capacity to determine the truth of, especially if the bombardment directly enriches the bombardier. Nor should society accept that "social media" through clever production ("Inszenierung") and manipulation of relationships multiply information of questionable veracity. The public should have a right to fully understand the business models, including the revenue streams of the various actors in cyberspace, so they can determine for themselves whether they want to serve as a (mostly free) resource. However, legal limits on these models will be difficult to enact because they are extensions of models that are as old as commercial mass communication and are deeply rooted in modern economies.

Finally, it is doubtful whether a decision of the Supreme Court meant to protect political speech ("Anonymity is a shield from the tyranny of the majority" and "protections for anonymous speech are vital to democratic discourse") should be used to provide a shield of anonymity to creators of fake realities [19]. Clearly, without knowing who the offender is, targeted individuals have little chance to seek redress, especially if, as is currently the case, law enforcement agencies have limited capacity to

support their efforts or to pursue offenders on their own. Other democratic countries have press laws that require that every publication identifies who is responsible for the content (e.g., [20]).

6.1.3. Threats to personal freedom and to property rights

Personal property, no matter how small that property might be, is the physical equivalent of privacy. Both, together, define personal freedom. A person deprived of all private property has lost the ability to express themselves in a space that is totally controlled by them. The object of this expression is formed in the space of privacy.

The process of expropriation of property and personal freedom through cyberspace is well advanced and will be difficult, if not impossible, to reverse. Any remedy will need to target the root of the problem: the ability of providers of services in cyberspace to collect and exploit personal data. This will stop the development of algorithms that create insight into a person's private space deeper than the person themselves possess. Breaking the monopolistic control of cyberspace by service providers appears to be a necessary first step. It will curtail their influence over the political process that supports the process of expropriation.

6.2. Threats to Businesses Users

Business users are on the opposite side of the coin from individuals. They benefit from the collection and analysis of private data of individuals. Their first attention will be to protect their physical ownership of their data through various security arrangements. This is where the technological parts of cybersecurity, algorithm-based measures, including encryption, have their place. This is the focus of an abundant collection of literature dealing with this.

6.3. Threats to Affinity Groups and Formal Social Organizations

Affinity groups and formal social systems are exposed to threats from cyberspace in ways analogous to those an individual is exposed to. Those threats are to their own sense of identity, their ability to keep information private, and their ability to chart their destiny as a group. Depending on designs of some anonymous institutions within cyberspace, they may be led to admit uncontrollable numbers of new members, or they may be moved to tighten their circle and form "Filter Bubbles." In the end, their filter bubble may be "weaponized" for political ends of the institution that fostered their establishment, or, through commercial arrangements, by some other institution. This may include battles with other filter bubbles directed by the same or different institutions.

Clearly, in any case, the group loses control of its identity and destiny. The end state may be much worse than it could be for individuals. However, the tools of control are similar. Consequently, the measures to protect against any threat will be the same as for individuals.

6.4. Threats to Sovereign States

Sovereign states are groups that control a specific territory and have dominion over their citizens. They issue laws and regulations to maintain social, economic, and political order within their territory; and to assure the freedom and safety of their citizens and properties owned communally and by individual citizens. Being sovereign, the state is free to arrange its affairs according to its preferences. And it is free to join other states to develop and implement common rules.

The threats identified for individuals and groups apply within the territory of a state. And any state should be free to shape measures of protection in accordance to the actual threat and their preferences.

Due to the transnational reach of cyberspace that developed in an opportunistic fashion over a large part of the world, sovereignty of states over cyberspace has been eroded without much public awareness. Sovereign states, therefore, find themselves in the situation described for affinity groups and formal social organizations. Increasingly, they find themselves victims of manipulation of their political, social, and economic affairs. Citizens are more closely connected to institutions in cyberspace than they are to the constitutional agencies in the state. For a state, regaining control of its sovereignty is a difficult undertaking because the interest of the state is positioned against the interest of a largely anonymous entity in cyberspace that controls the opinions, if not the minds, of a large segment of the population. For the state to succeed in this confrontation, it must use the facilities of cyberspace that are controlled and protected by institutions that may be largely outside the domain of the state. And those institutions may be beholden to other sovereign states which may have their own designs for the state's evolution. This will require delicate diplomacy. Also, since service providers are contributing their entire revenue to the growth of the state's economy, curtailing them would violate the ethical principle that is currently driving the economy, and would be seen as hurting the interests of the state. [21].

In any case, if the state wants to retain control of its future, it has no choice but to take over full control of cyberspace as it applies to its territory and citizens. This will require active control of all transborder traffic of information to assure that it meets at least the standards for intra-state traffic. This includes the design and application of algorithms and other systems and processes. The state also needs to assert that any interference in the internal affairs of a sovereign country is a violation of international law.

6.5. Threats to the Global Human Sphere

What distinguishes the human sphere from a simple accumulation of individuals, or even groups or sovereign states is that there is nothing beyond it. Humans being inside it, according to Wittgenstein, cannot control it, since that would require them to be outside it, a logical impossibility [22]. Similarly, as cyberspace, which is inside the human sphere, approaches the limits of the human sphere, it will elude human control – a stark prospect, since the rate of growth of cyberspace seems to make that inevitable in the not too distant future.

Clearly, the human sphere and cyberspace are not defined in physical terms alone. According to Teilhard de Chardin, the human sphere includes the noosphere, which is the locus of human introspection [23]. This is where human evolution is currently focused. It is also where much of cyberspace is located. Extrapolating from the above discussion about cyberspace increasingly extracting from humans that which is the essence of humanness, as cyberspace covers the entire human sphere, there will be no humanness left. This will be the end of humanity, at least as we know it. Humans will have lost control over the system they themselves created. And there will be no return from this state.

There have to be limits on the kind of experimentation with, and instrumentalization of human minds and freedoms. It is difficult to see why a process like the Institutional Review Board (IRB) process required for experiments with human subjects cannot equally be applied to experiments in the infinitely larger domain of cyberspace. Beyond that, there are all the measures that have been outlined in this paper that, combined, would be a foundation for effective control.

7 Obstacles to a Sustainable Cyberspace

Unfortunately, implementation of this proposal would face vehement opposition from a number of directions. And as the dominance of the human sphere by cyberspace increases, the ability to overcome the opposition would diminish. It will be those who oppose reform who will seize control over

cyberspace and through it over an expiring humanity.

There are three main sources of obstacles to effective control of cyberspace: military and national security interests, the community of businesses benefitting from the current situation of cyberspace, and ethical norms governing the human sphere. Of these, military and national security interests are most powerful and overwhelm the others.

Even if a military strategy for operations in cyberspace is meant to be truly defensive, the military will be tempted to follow the adage that the best defense is a good offence. In a world of several superpowers, even if one power intends to act purely defensively, it needs to match the aggression of other powers to avoid losing. This is setting up cyberspace as a permanent battlefield, which only ends when one of the parties has reached total dominance – or all are exhausted. As Gen. Paul M. Nakasone, the head of the US Cyber Command (which was upgraded to a Unified Combat Command in May 2018) articulated: "If we are only defending in 'blue space,' we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries" [24]. Clearly, this eliminates the possibility of any part of cyberspace remaining outside the battlefield.

As recurring reports of cyberattacks conducted by various government agencies indicate, a cyberwar is in full progress (see e.g., [25]). In other words, military and national security organizations are functioning like the "bad actors" that cybersecurity intends to defend against. The end-state they are working toward is nothing less than what we have defined as the end of humanity. Unless some way can be found to end this cyber war, the military and national security agencies cannot but oppose the proposals developed in this paper.

8 Summary

Following the paradigm of purposeful systems, we have framed cybersecurity as part of the global sustainability equation. We have outlined measures that could stop the threat. The measures focus on legal and institutional issues. They presume the existence of a stable infrastructure that is secure against attacks. However, military and national security agencies' use of cyberspace is following paths that are directly opposite to the proposed measures. This paper, therefore, concludes that in order to maintain sustainability of the human sphere it is necessary to end the cyberwar that is already in full progress. Urgency is indicated because many of the conditions created in cyberspace are becoming increasingly irreversible.

References

[1] J. Clough, *Principles of Cybercrime*, 2nd ed. Cambridge: Cambridge University Press, 2015.

[2] Etschmaier, Maximilian M., "Purposeful Systems: A Conceptual Framework for System Design, Analysis, and Operation," *Int. J. Comput. Their Appl.*, vol. 22, no. 2, pp. 87–100, Jun. 2015.

[3] M. Gorham, "2018 Internet Crime Report," Federal Bureau of Investigation, Internet Crime Complaint Center 2018, Internet Crime Report, Washington, DC, Annual Report, 2018.

[4] N. Perlroth and S. Shane, "In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc," *New York Times*, 26-May-2019.

[5] "FBI Cyber task Ransomware_Trifold_e-version.pdf.".

[6] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, p. 9, 2014.

[7] E. Ostrom, *Governing the Commons*. Cambridge University Press, 2015.
[8] D. K. Mulligan and F. B. Schneider, "Doctrine for Cybersecurity," *Daedalus*, vol. 140, no. 4, pp. 70–92, Oct. 2011
[9] J. Mayer, "How Russia Helped Swing the Election for Trump," *The New Yorker*, 24-Sep-2018.
[10] M. M. Etschmaier, "Can Humans Stay in Control of Systems They Create?," *Int. J. Comput. Their Appl.*, vol. 24, no. 4, pp. 149–154, Dec. 2017.
[11] Stanford University, "2019 Commencement address by Apple CEO Tim Cook," *Stanford News*, 16-Jun-2019. [Online]. Available: https://news.stanford.edu/2019/06/16/remarks-tim-cook-2019-stanford-commencement/. [Accessed: 17-Jun-2019].
[12] O. Schwartz, "Deepfakes aren't a tech problem. They're a power problem," *The Guardian*, 24-Jun-2019.
[13] M. M. Etschmaier and G. Lee, "Defining the Paradigm of a Highly Automated System that Protects Against Human Failures and Terrorist Acts and Application to Aircraft Systems," vol. 23, no. 1, p. 8, 2016.
[14] M. M. Etschmaier and Gordon K. Lee, "Designing Secure Computer Systems as Purposeful Systems," *IJCA*, vol. 23, no. 2, pp. 105–115, Jun. 2016.
[15] M. M. Etschmaier, "Designing an Ethical System of Global Sustainability as a Purposeful System: GEBAT, Global Equity of the Burden Added Tax," Int. J. Sustain. Policy Pract., vol. 14, no. 1, pp. 17– 35, 2018.
[16] F. S. Nowlan and H. F. Heap, *Reliability-centered Maintenance*. San Francisco: Dolby Access Press, 1978.
[17] A. C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days," *The Atlantic*, 01-Mar-2012. [Online]. Available: https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-youencounter-in-a-year-would-take-76-work-days/253851/. [Accessed: 08-Jul-2019].
[18] S. Powers, "Where did the principle of secrecy in correspondence go?," *The Guardian*, 12-Aug-2015.
[19] *McIntyre v. Ohio Elections Commission*. 1995.
[20] A. Unternehmensberatung, "§ 118 StGB (Strafgesetzbuch), Verletzung des Briefgeheimnisses und Unterdrückung von Briefen - JUSLINE Österreich." [Online]. Available: https://www.jusline.at/gesetz/stgb/paragraf/118. [Accessed: 08-Jul-2019].
[21] M. M. Etschmaier and G. K. Lee, "Integrating Humans and Machines into Purposeful Systems that Keep the Human in Control," Int. J. Comput. Their Appl., vol. 23, no. 2, pp. 55–168, Dec. 2017.
[22] L. Wittgenstein, Tractatus Logico-Philosophicus. Cosimo Classics, 2007.
[23] P. Teilhard de Chardin, *The Phenomenon of Man*. New York: Harper and Row, 1975.
[24] P. M. Nakasone, "A Cyberforce for Persistent Operations," *Jt. Force Q.*, no. 92, pp. 10–14, 2019.
[25] A. Press, "US launched cyberattack on Iranian rockets and missiles – reports," *The Guardian*, 23-Jun-2019.

Acknowledgements

The author thanks Judson MacLaury for the skillful professional editing, Gordon Lee for suggesting and help in framing this paper, and Christoph M. Etschmaier for research and editorial assistance as well as valuable discussion of the conclusions.