



Cyberpandemics

Jeffrey Voas, IEEE Fellow

Phil Laplante, Penn State

Cyberpandemics share similarities with biological pandemics, and we all have a role to play in preventing both.

are not sensationalizing the CV tragedy. Rather, we hope that revisiting the article might put the current pandemic into a perspective that can help us learn how to better deal with

Each year, Google announces what the most popular search term was from the previous year; *Disney Plus* was the top searched term on Google in the United States for 2019.¹ Given current events, we wonder if any of the following terms will become the most popular for 2020: *pandemics*, *coronavirus*, *COVID-19*? We ponder this because it appears from media reports that public acceptance of global pandemics may have become a new “normal” threat. Although global pandemics have been discussed on television and in movies for years, they have had somewhat of a science fiction angle to them even though they occurred often in past centuries.

More than 10 years ago, a few of us discussed out-of-the-box ideas, such as “what if the power grid went completely down?,” “what if the banks fail, and no one can access cash from an ATM?,” and “what if society completely or partially shuts down from a global cyber event?” In a 2009 article, we discussed various scenarios of the last idea.² The events of the coronavirus (CV) pandemic over the past few months have made us rethink that article. Note: we

future biological viruses and avoid cyberpandemics.

So, what is a *cyberpandemic*? Quite simply, it is a massive disruption of computing service that triggers second- and third-order failures of computing and noncomputing systems worldwide. Consequences could include widespread failure or malfunctioning of critical infrastructure systems and the associated major societal damage. Perpetrators of cyberpandemics could include rogue governments (or elements therein), terrorist groups, corporations and consortia (that may profit from the pandemic’s affects), malicious actors (of varied motivations), individuals, or even an accident (for example, a weaponized malware gone awry). As far as we know, a cyberpandemic has never been successfully perpetrated, but we all know that the weaponization of cyberspace is very real. A full potential of that is yet to occur.

The conditions that could lead to a cyberpandemic are similar or analogous to those for a biological pandemic: human complexity, attack multiplicity, and delayed effects. In the cyber world, human complexity is represented by people “packed too tightly in cyberspace” and the resultant complex social interactions online. Attack multiplicity means that the attack involved multiple

Digital Object Identifier 10.1109/MC.2020.2984253
Date of current version: 4 June 2020

IN THIS ISSUE

Parhami, the author of "Reliability Inversion: A Cautionary Tale," explains the notion of "reliability inversion." He claims this phenomenon occurs in practice for actual systems under realistic assumptions and points to certain system architectures that are more amenable to producing tight reliability bounds with tractable analytical models or simplified simulation-based models. An example involving centralized versus distributed reconfiguration switching in 2D processor arrays is used to support the ideas with quantitative results.

In "An Enterprise Transformation Guide for the Inevitable Blockchain Disruption," Demir et al. present a methodology termed the *blockchain technology transformation framework* (BTTF). The article claims that this approach can inform decision makers on how blockchain fits in their processes, what data will be in their transactions, and who the participants will be. This framework builds a design map by which process

owners can analyze the suitability of blockchain technology. Through this approach, the authors believe that BTTF can provide organizations with a way to redesign their processes or identify opportunities for using smart contracts. Use case examples in supply chain and real estate are provided.

The last article in this issue is "Is Privacy Regulation Slowing Down Research on Pervasive Computing?" Bettini et al. present a study that investigated the impact of the recent evolution of personal data protection legislation on researchers in mobile and pervasive computing. The authors gathered feedback from more than 150 researchers in this field to better understand if this attitude is shared. Their findings indicate that most respondents do not feel there are any major impediments in adhering to privacy regulations, and they also found that the respondents were somewhat familiar with the latest legal developments and the majority seemed to be in favor of clear and strict privacy regulation.

Digital Object Identifier 10.1109/MC.2020.2988546
Date of current version: 4 June 2020

– Jeffrey Voas, Editor in Chief

simultaneous attacks and used more than one orthogonal (computer virus) vector mechanism. These may include one or more noncyber components in the attack. In the human analogue, this is somewhat equivalent to a virus that attacks the immune and nervous systems. In a cyberpandemic, attackers could launch the attack by using a noncyber component as a diversion, to soften the environment for the attack, or as the trigger mechanism, to signal the start of the attack or disrupt society's ability to recover. Social networks increase the likelihood of people falling into traps, can be used to create diversions for an attack (for example, flash mobs and riots), and can propagate or trigger malware. Delayed effects mean that symptoms emerge long after infection has occurred, making widespread dispersal likely and difficult to prevent.

In 2009, we introduced five potential scenarios for cyberpandemics; space in this editorial precludes reviewing them, but one such scenario (wag the dog) involved exploiting some type of natural disaster (such as a human pandemic) to distract attention from the impending threat as well as tire and weaken response agencies before the launch of a cyberpandemic. In fact, on 18 March 2020, a cyberattack was launched against the U.S. Department of Health and Human Services, apparently, to prevent the agency from responding to the CV. The origin of the attack is still unknown,³ and this attack did not reach the scale of a cyberpandemic. The point here is simple: a biological virus can greatly impact global economics and financials; however, an attack on the cyber infrastructure can also affect human health outcomes, for instance, holding

hospitals hostage via ransomware or completely shutting down the supply chains that medical professionals rely on.


As we write this editorial (in mid-March), the final toll of the CV is unknown, and we hope it will soon be conquered. But what is clear is that everyone must help fight this and future biological pandemics.

However, nations, organizations, and individuals also have a role to play in preventing cyberpandemics. The role of nations and groups of nations is clear. The role of individuals is also clear—as with biological pandemics, each person has a role to play in cyberspace by applying the principles of 1) least exposure, 2) defense in depth and separation of privileges, and 3) being aware of "dry runs" and probing activities and reporting them. Charitable, business, and professional

organizations also have a role, and we can marshal their forces to help.

We call upon members of the IEEE Computer Society to consider future research efforts on

- › telemedicine, the Internet of Things, and enabling technologies
- › big data, data analytics, and visualization
- › high-performance, cloud, fog, and edge computing (to support pandemic concerns)
- › human-computer interaction and the appropriate interfaces
- › social networking, communication protocols, and related psychosocial aspects
- › reengineering and rethinking education for virtual delivery (for example, clinicals, labs, and internships).

There are many others that we are missing in this short list. Not coincidentally, all of these are areas of interest to the IEEE Computer Society and *Computer*. Stay well. 

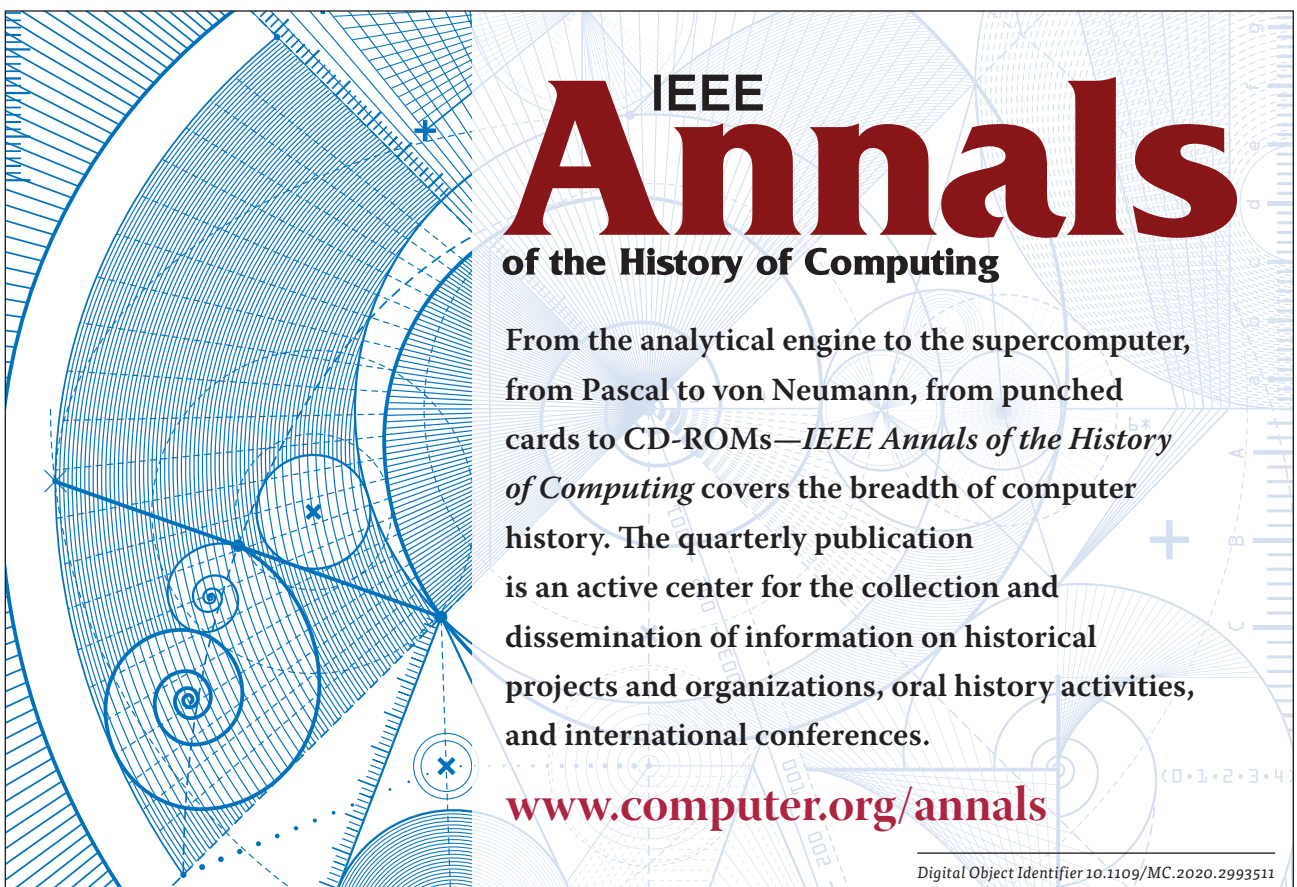
REFERENCES

1. J. Moreno, "These were the top Google searches and trends of 2019," *Forbes*, Dec. 29, 2019. [Online]. Available: <https://www.forbes.com/sites/johanmoreno/2019/12/24/these-were-the-top-google-searches--and-trends-of-2019/#625c7ee43089>
2. P. Laplante, B. Michael, and J. Voas, "Cyberpandemics: History, inevitability, response," *IEEE Security & Privacy*, vol. 7, no. 1, Jan./Feb. 2009, pp. 63–67. doi: 10.1109/MSP.2009.4.
3. H. Samsel, "Cyber attack hits Department of Health and Human Services amid government coronavirus

response," *Security Today*, Mar. 18, 2020. [Online]. Available: <https://securitytoday.com/articles/2020/03/18/cyber-attack-hits-department-of-health-and-human-services-amid-government-coronavirus-response.aspx>

JEFFREY VOAS is the editor in chief of *Computer*. Contact him at j.voas@ieee.org.

PHIL LAPLANTE is a professor of software and systems engineering at Penn State and a member of the *Computer* editorial board. He is a Fellow of the IEEE. Contact him at plaplante@psu.edu.

The graphic features a complex, blue-toned background with geometric patterns, including a large spiral on the left and various circular and linear elements. The IEEE logo is positioned above the main title.

IEEE Annals

of the History of Computing

From the analytical engine to the supercomputer, from Pascal to von Neumann, from punched cards to CD-ROMs—*IEEE Annals of the History of Computing* covers the breadth of computer history. The quarterly publication is an active center for the collection and dissemination of information on historical projects and organizations, oral history activities, and international conferences.

www.computer.org/annals

Digital Object Identifier 10.1109/MC.2020.2993511