A PUBLICATION OF THE NATIONAL ASSOCIATION FOR COURT MANAGEMENT
Court Manager Vol. 34 #4 – Winter 2019


COURT MANAGER

# Courts Have a Significant Role to Play in the Whole-of-Government Approach (WGA) to Our Safety and Security*

*by* INGO KEILITZ, KATHARINE W. JENNINGS, SUSAN A. EHRLICH, CAROLINE N. BROUN, KATHRYN H. FLOYD & MICHAEL L. BUENGER
NOV 2019

Share this article

Courts must get ready for a riskier world today. We and, therefore, they face unprecedented threats to our safety, security, and welfare, including natural disasters, pandemics, terrorist attacks, biological and chemical attacks, and cyberattacks by increasingly sophisticated adversaries using not only weapons of mass destruction but also weapons of mass disruption. Such threats and others discussed in this article warrant the attention of courts and their justice partners, not just to mitigate the risks to the continuity of their own operations but also to protect society as a whole.

During and after the war in Kosovo (1998-99), the courts in Kosovo lost some of their case records, including case registers and case files.[1] When the Kosovo courts resumed operations after the war, court staff inventoried and compared the case files against the case registers. They found that case files were lost or missing during the withdrawal of the Serbs from Kosovo. Most of the missing records were civil-case files, predominantly inheritance and property-dispute cases. The land

registry books in Kosovo were taken by the outgoing Serbian regime and were never returned to Kosovo. In 2013 the Serbian government agreed to provide copies of land registries but not the original records. To date, some of those records have been delivered, but the vast majority are still missing, creating a backlog of cases that the courts cannot decide or adjudicate fairly. All parties to a dispute have records claiming ownership. All documents are authentic, one set issued by the Government of Kosovo, the other set by the Government of Serbia. What documents are accurate when there are no land registries to determine the history of a property, for example? What can courts do when the property has been sold and resold multiple times to different parties, and yet there is another party claiming ownership?

What occurred in Kosovo is an example of what can happen when a court system's records vanish, as occurred in the aftermath of the civil war between Kosovo and Serbia, undercutting history, finality, reliability, and certainty. What was considered settled, e.g., the existence or the acquittal of a crime, the ownership of a house, the parentage of a child, finality of a separation or divorce, recompense for a wrong, the existence of a business, the nature of a contract, and the presence of civil rights, becomes unsettled. This unsettling of individual cases has occurred, and will occur, and not just in the context of war, although the impact usually is limited and confined to the parties in individual cases. Certainly, courts have mechanisms to settle issues in individual cases and to reestablish finality and reliability through various procedures. However, what happens when the court data loss is on a massive scale? When thousands or millions of court records are compromised or lost, when people can no longer rest on what was predictable and reliable? The settled is unsettled; the reliable becomes unreliable. Social cohesion frays. Bad actors take advantage of the ensuing political, social, and economic chaos.

More recently in May and June 2019, the computer systems of two courts in the United States were crippled. The computer network that supports the Georgia state court system was taken offline by court officials following a ransomware cyberattack in late June (Murdoch, 2019). Ransomware is a type of malware, software that is designed to disrupt, damage, or gain unauthorized access to a computer system, encrypting computer files until a sum of money is paid, usually in Bitcoin or another cryptocurrency because it is difficult to trace.

Officials of the First Judicial District Court in Philadelphia reported that the court's websites and computer programs were shut down as a precaution after a virus was found on a limited number of computers. In response, the court's website, employee email accounts, and electronic filing (e-file) were temporarily suspended (Shaw, 2019). The shutdown disrupted civil cases more than criminal ones. Online criminal dockets, which are on a statewide system, were still accessible. But the online civil-docket search was not functioning. Law firms that handle civil cases had to resort to hand delivery by court employees or bike couriers to file motions and other documents. More than a week after the attack, there still were no answers as to why it happened, when it would be fixed, or how much it would cost, not only to the court but also to those who were affected. To safeguard other systems in Philadelphia, including that of the courts, the city's Office of Innovation and Technology "shut down certain court IT functions to fully review and clean the operating systems," a city spokesperson said.

These are examples among the growing threats of cyberattacks and hefty ransomware demands facing United States' institutions and cities, states, and other political divisions. Cyber criminals exploit vulnerabilities in state and local governments' aging computer systems. Once the malware infects a computer, it encrypts files and spreads into an entire network to infect more and more machines in a court's computer system. Governments, especially courts, have limited resources to attract cybersecurity experts. In the past, ransomware attacks were mostly limited to individual computers. Now hackers are going after larger targets such as governments, including court systems (Calvert and Kamp, 2019: A3), many of which are unable to afford to pay at least the initial ransom demand or unwilling to give in to extortion.

# Broader Response Needed

As the Kosovo, Georgia, and Philadelphia cyberattacks illustrate, determined state-sponsored or private adversaries can debilitate a nation-state, affecting, perhaps catastrophically, its residents, its economy, and its institutions without the use of deadly force. In the United States, much of the responsibility for preparedness and response to threats to security and safety falls to state and local public-health practitioners, law enforcement, and emergency responders. In transnational threats, responsibility falls to the military and intelligence community. We contend that such threats to our safety and security require a much broader approach, and a higher level of urgency and cooperation, including rapid and honest communication, broad coordination, collaboration, and responses across all three branches of government–executive, legislative, and judicial–as well as nongovernmental agencies, an approach referred to as a Whole-of-Government Approach (WGA).

The WGA is rooted in commonsense assumptions, most notably that the complex and intractable problems of national and transnational safety and security that we explore in this article defy solutions by the actions of just one or two government entities, such as the military and intelligence communities. Rather, a WGA stresses the principle of unity of action and the importance of all interagency and coalition partners coordinating their respective efforts (White, 2014).

**Box 1. Stephen Hawking on Why a WGA Response Is Hard Today.** Stephen Hawking, the world-renowned physicist and cosmologist, worried about the size and complexity of the perils that humanity faces and our limited individual knowledge of solutions. In his posthumously published book, *Brief Answers to Big Questions*, he

addressed the question: “Will we survive on earth?” He believed that we now have the technological power to destroy every living creature on earth. The “threats are too big and too numerous,” including global warming, disease, famine, nuclear war, autonomous weapons, and decimation of animal species, he writes (Hawking, 2018: 147). At the same time, our store of information in books and other forms of storage has grown exponentially, and the time scale of accumulation of even more information has shrunk over the last 300 years. This has brought unimaginable benefits, but the evolution of our record of information and knowledge is severely limited by two factors: the complexity of the intractable problems we face around the globe (see United Nations, Sustainable Goals) and the hyper-specialization of knowledge and expertise of the problem solvers. No one person today can be a master of more than a tiny corner of knowledge. And the more complex the problem, the more unlikely it is that one person or even one group of persons can solve it. This is an area where quantum-computer power could help in the future (five years?) by combining knowledge across multiple disciplines into a single artificial intelligence system. For a benign example, Alexa, Siri, Watson, and other digital assistants with access to information in many areas could help us solve our problems that people with a narrow range of expertise cannot.

# Unprecedented Threats

The 21st-century threats to our homeland security are more diverse and serious than ever and affect every aspect of our lives directly or indirectly (White House, 2019). The threat landscape spans natural and manmade disasters; epidemics and pandemics[2]; chemical, biological, radiological, nuclear, and explosive (CBRNE) attacks; cyber incidents and espionage; transnational criminal organizations’ operations; and violent conflicts (see figure below; White House, 2017b; Pickart, 2018; Coats, 2019; ASPR, 2019). Discussing each type of threat illustrated in Figure 1 is beyond the scope of this article, but a brief description of the threats and hazards we face today bears a comment or two.

**Examples of 21st Century Threats**




The biggest driver of change today is technology. Advances promise to change our lives for the good and, at the same time, raise the specter of doom. This duality is problematic in categorizing and defining the threats in Figure 1. For instance, the rapid and global advances in genetic engineering and synthetic biology hold great promise for the development of life-saving therapies, but these same tools in the hands of terrorists can be used to create deadly weapons with the potential to inflict enormous harm on public health, safety, and security, including economic security (ASPR, 2019: 5; White House, 2018a: 4).

The threats are not hyperbole. In recent years, several chemical weapons attacks and emerging infectious disease outbreaks (i.e., newly appearing in a population) garnered global media attention. In 2013 and 2017, sarin attacks in Syria killed a total of more than 1,400 people (Barnard and Gordon, 2017; Bauer, 2019). There was a sarin attack in the Tokyo subway in 1995. Subsequent deadly chemical-weapons attacks involved chlorine gas, sulfur mustard, and assassinations with the nerve agents VX and Novichok (Coats, 2019; White House, 2018c).

The two largest Ebola outbreaks ever recorded occurred and continued during the same time frame. Both the 2014-2016 outbreak in West Africa and the ongoing 2018-2019 outbreak in the Democratic Republic of the Congo (DRC) were declared a “public health emergency of international concern” by the World Health Organization (WHO), indicating that the disease outbreak is serious, poses international public-health risks, and requires an international response (WHO, 2014, 2016a and

b, 2019). In the United States, public officials, including judges in several states, had acted to curtail the spread of Ebola in this country when 11 individuals who were infected or who had been exposed to Ebola returned to the United States in 2014-2016 (CDC, 2019a). Similarly, judges in several states tried to contain the alarming outbreak of measles, which had already affected 1,164 individuals in 30 states, the largest number of cases in the United States since before the disease was declared eliminated here in 2000 (CDC, 2019b).

Even the frequency and intensity of natural disasters such as droughts, floods, tornadoes, hurricanes, and downpours are increasing (ASPR, 2019). As we wrote this article in the summer of 2019, broad swaths of the United States from California to New Jersey were hit by a record-breaking number of devastating tornadoes. At the same time, millions of people were enduring hurricanes, extreme heat, unremitting rainfall, and destructive flooding. The threats of such natural disasters, as well as pandemics, epidemics, and terrorist attacks, including cyberattacks, demand a coordinated and rapid response by many actors from dozens of governmental and nongovernmental entities.

In this article, we will focus our discussion primarily on the CBRNE and cyber threats (see Figure 1) to illustrate the risks to public health, safety, security and our way of life and the potential role of the third branch of government in preparedness, response, and resilience. For most of these threats, we cannot anticipate whether and how courts will be called upon to respond, but the risks and threats indicate the necessity for advanced planning, education, and coordination well before court decision making is required.

# An Analytical Framework

We construct an analytical framework for considering how the participation of the third branch of government and its justice institutions, especially courts, in a Whole-of-Government approach (WGA) is viable. By what means can courts embrace a WGA without undermining their independence and thereby tilting the balance of power to the executive and legislative branches, a development antithetical to liberal democracies and to the United States Constitution's framework of the separation of powers? The purpose of this article is to illuminate and prompt serious conversations about this question among court administrators, judges, and policymakers–including federal, state, and local agencies, and elected officials.

After examining the types of threats and risks we face today–some of which are existential–and defining WGA, we explore how a WGA, with its demands for speed, expedition, and joint action, runs counter to the doctrines of judicial independence; the separation of powers of the judicial, legislative, and executive branches; and the checks and balances among them, ideals and principles that are fundamental to the governance of democratic countries and institutions. We then identify several developments, such as the courts' increased public engagement, and offer several arguments (e.g., that the separation of powers of the three branches of government is not intended to be absolute) that are favorable to judicial systems' active participation in WGA.

In conclusion, our assertion in the article's title is our strong belief, reached by consensus, that for the security and safety of users and employees of courthouses, for the good of the communities they serve, and for the good of society as a whole, the leaders and managers of national and subnational justice systems should become active participants in a WGA response to the risks and threats we discuss.

# Definition of a Whole-of-Government Approach (WGA)

"Whole-of-Government," as defined by the assistant secretary for preparedness and response (ASPR) in the United States Department of Health and Human Services, "refers to public service agencies working across portfolio boundaries to achieve a shared goal and an integrated government response. Approaches can be formal and informal and include government partners at federal, state, tribal/territorial, and local levels" (ASPR, 2019: 9). The first mention of a WGA, then referred to as "joined-up-government," was made in Tony Blair's administration in the United Kingdom (British Broadcasting Corporation, 1998). Variously termed "one-stop government," or even more expansively, a "whole-of-community response" and a "whole-of-society approach" (Realuyo, 2019: 137, 141), WGA represents a change of emphasis away from single-purpose organizations, departmentalism, and disaggregation hampering an integrated and coordinated approach to addressing complex societal problems (Richards and Kavanagh, 2001).

The WGA is a flexible concept. It encompasses efforts to bring together, integrate, and synchronize all the different tools in the national-security toolkit to advance a nation's security interests. This includes the balanced use of the military, diplomatic corps, economy, information, and intelligence community, and more as appropriate, to a challenge or opportunity at the federal, state, and local levels of government. A WGA helps strategic leaders think about problems in complex ways from a variety of perspectives with a broad and deep understanding of the authorities and cultures of their interagency partners.

Of course, a nation's security interests reach beyond national boundaries. Few threats stay confined within the boundaries of any one country. Transnational intelligence sharing, for example, is in the national interest, especially to address risks during fast-moving events.

In a society where effective governing and problem solving are hindered by systemic disconnection among government agencies, how do we encourage interagency cooperation to better address national-security challenges? In April 2018, the William & Mary (W&M) Whole of Government Center of Excellence (see Box 2) held its Inaugural National Security Conference to address that question (Terry et al., 2019). In his keynote address, Russell Travers, acting director of the National Counterterrorism Center, explained the evolution of national-security threats and the need for improved interagency operations. “The downsides of globalization pose a significant challenge to our national security apparatus: individuals and networks can have strategic impact; problems straddle foreign and domestic lines; and threats transcend departmental and agency responsibilities. ‘Whole of Government’ solutions are more critical than ever before. We have to work much closer together than we have in the past.” Travers identified three necessities for combating our country’s national-security challenges: more effective interagency cooperation than in the past; greater involvement of the private sector; and importantly, increased WGA training and education.

Another conference speaker, Michael Findley, professor of government, University of Texas at Austin, and co-director of its Innovations for Peace and Development Program, reviewed the latest research on the impact of foreign aid on conflict and peacebuilding. He averred that the biggest challenge to cooperation lies in the frequent disconnect between an organization’s headquarters and realities in the field. To close that disconnect, another conference speaker, Ronald Neumann (ret.), president, American Academy of Diplomacy, former ambassador to Algeria, Bahrain, and Afghanistan, and former deputy assistant secretary of state, stressed the importance of improved training for civilians to learn how to put their cultural and political knowledge to work on the ground to bridge political, cultural, and military divides. At the same time, he added, the military needs to more effectively use civilian input in the field.

**Box 2. The Whole of Government Center of Excellence**
The William & Mary Whole of Government Center of Excellence is an interagency policy center that focuses on research, education, and training to address complex national-security problems. It promotes interagency collaboration across the different organizational cultures that must be harmonized to facilitate true interagency collaboration. It serves as a convener of representatives of federal, state, and local governments, as well as nongovernment stakeholders. The center’s mission is to provide practical training on interagency collaboration, complex national-security and other public-policy problems, and to support research into the WGA solutions. It brings together leaders from all levels of government and the military for symposia, discussions, and projects to promote creative, collaborative research and solutions to emerging issues (Terry et al., 2019).

In December 2017, President Donald J. Trump announced a new national-security strategy rooted in WGA. Then Defense Secretary James N. Mattis called the strategy “clear and comprehensive” (Garamone, 2017).

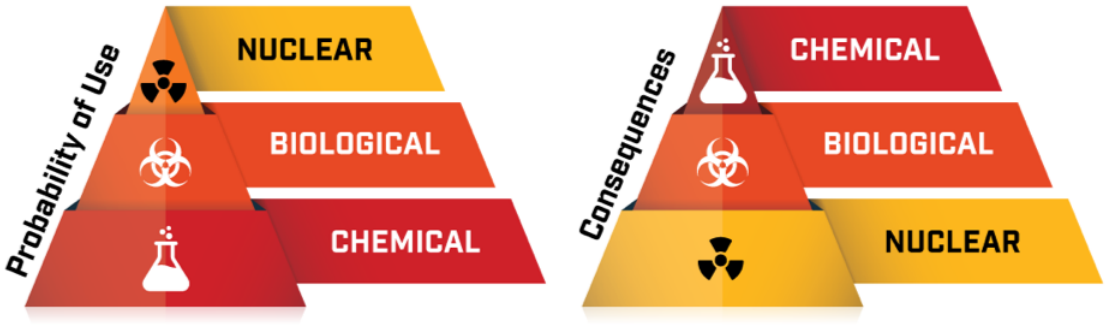
# Risks, Threats, and Challenges

> The strategic environment is changing rapidly, and the United States faces an increasingly complex and uncertain world in which threats are becoming ever more diverse and interconnected.
>
> *Daniel R. Coats, 2019*

## Biological, Radiological, Nuclear, and Explosives (CBRNE) Attacks

In a risk assessment of public-health-disaster scenarios, the New York City Health Department (NYCHD) compared the severity and probability of various threats (Pickart, 2018) and determined that the two variables were often inversely related. In terms of CBRNE, as one example, a chlorine gas release (chemical) was determined to be more probable but less severe than a biological or nuclear attack. Alternatively, an improvised nuclear device was determined to be the most severe but least probable disaster scenario. However, when the NYCHD accounted for the impact of planning on the various risks, pandemic influenza and aerosolized anthrax were ranked higher priorities than chemical or radiological/nuclear risks. Former Director of National Intelligence Daniel R. Coats recently issued the following warning: “We expect the overall threat from weapons of mass destruction (WMD) to continue to grow during 2019, and we note in particular the threat posed by chemical warfare (CW) following the most significant and sustained use of chemical weapons in decades” (Coats, 2019). Bad actors intent on using weapons of mass destruction have numerous choices from

**Probability Versus Severity of Nuclear, Biological, and Chemical Attacks**






the widely available toxic industrial chemicals to traditional chemical weapons, natural and synthetic biological agents, and nuclear or radiological materials (White House, 2018c).

According to the United Nations Office for Disarmament Affairs (UNODA), “nuclear weapons are the most dangerous weapons on earth” (see UNODA, “Nuclear Weapons”). The multilateral Treaty on the Non-Proliferation of Nuclear Weapons was entered into force in 1970 and since has a total of 191 signatory states. The treaty affirms the benefits of peaceful uses of nuclear technology, notes the extreme dangers of nuclear war, and provides safeguards against such proliferation. There also are the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (commonly known as the Biological and Toxin Weapons Convention, or BWC) and the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (commonly known as the Chemical Weapons Convention, or CWC), which address the extreme dangers of certain biological and chemical weapons.

Despite these and other treaties and safeguards, the threats of misuse from states and terrorists persist, and new and emerging technologies continue to change the landscape (National Nuclear Security Administration, 2018). The National Strategy for Countering Weapons of Mass Destruction Terrorism reports that dangerous amounts of nuclear, radioactive, biological, and chemical materials suitable for weapons development have been found outside regulatory control on multiple occasions (National Nuclear Security Administration, 2018; White House, 2018c). Russia, China, Pakistan, India and, potentially, Iran continue development of their nuclear weapons capabilities (Coats, 2019). North Korea may be readying the same (Albert, 2019). In regions of violent conflicts and political instability, controlling nuclear, radioactive, biological, and chemical materials is a challenge, and ensuring that these materials are not available for nefarious uses is a key tenet of counterproliferation measures (National Nuclear Security Administration, 2018; White House, 2018c).

Biological incidents, whether from emerging infectious diseases, pandemics or bioterrorism, from natural or synthetic derivation, are a particular cause for concern because of the potential for catastrophic consequences, including deaths, disease, psychological trauma, environmental impacts, and economic losses (White House, 2018a). Biological agents are unique in that many can proliferate after release, may not be initially detectable, may not have medical countermeasures, and are frequently transmissible–all of which greatly increases the hazard. The threat as well as the reality of rapid and widespread emerging pathogens is growing as societies become more mobile and populous, and as they encroach on human and wildlife habitat (White House, 2018a).

Today’s CBRNE threat landscape also reflects the elevated role of technology and the reduced barriers to existing and new technologies (White House, 2018a). The rapid advancements in genetic engineering, genome editing, and synthetic biology offer new medical countermeasures, vaccines, treatments, and personalized medicine, but they also present the risk of creating new or re-creating eradicated pathogens and toxins and modulating human physiology for negative effects (White

House, 2019). Moreover, the landscape of threats has expanded greatly due to the combination of enabling technologies and the multidisciplinary nature of biological research today (National Academies, 2018; *Economist*, 2019a and b; see Box 3).

**Box 3. The Columbian Exchange, Synthetic Biology, and Weaponizing Diseases.**
In the 15th and 16th centuries, after Christopher Columbus's 1492 voyage, there was a widespread transfer of horses and cattle, plants, culture, and human populations, as well as communicable diseases referred to as the Columbian Exchange (Crosby, 1972). Native Americans died by the thousands of imported Old World diseases such as measles, mumps, smallpox, typhus, and influenza. In an early example of biological warfare, the British military sought to infect Native Americans with smallpox, with some success, by giving them blankets and handkerchiefs from smallpox patients (Christopher et al., 2018: 3). The Europeans further weaponized this catastrophe by conquering the lands from those depleted and killed by disease.

Synthetic biology could design and recreate a weapon, such as smallpox or other orthopox virus, to weaken, incapacitate, or kill. In a controversial synthetic biology experiment in 2018, researchers described the creation of an infectious horsepox virus from chemically synthesized DNA (Noyce, Lederman, and Evans, 2018). This study provided an example of a new method that may lower the barrier to the synthesis of the variola virus, which causes smallpox. The study reignited the debate about dual-use research of concern (DURC), its requisite oversight, and limitations on publishing such research (Koblentz, 2018; Osterholm and Olshaker, 2017; NSABB, 2006, 2007).

## Cyber Threats

In today's modern world, cyberspace touches every aspect of our lives–commercial and financial, social, and political, to name a just a few. As our reliance on cyberspace grows, so do our vulnerabilities. Cyberattacks are occurring with increasing frequency and sophistication (White House, 2018b; Carlin, 2019; Lin, 2019). In August of 2019, the United States Department of Homeland Security issued a "Ransomware Outbreak" warning to municipalities and private organizations that "ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks" (Janofsky, 2019b: B4).

China, among other nations, has stolen trillions of dollars' worth of intellectual property through cyberespionage. Terrorists and other criminals have recruited members, raised money, and launched attacks using cyberspace (White House, 2018b). Russia continues to influence political perceptions, racial tensions, and trust in authorities through social-media operations, also called influence campaigns (Coats, 2019).

In their 2019 book, *The Fifth Domain,* Richard A. Clarke and Robert K. Knake, counterterrorism officials in several United States administrations, argue that cyber, the "fifth domain," is different from the other four domains–land, sea, air, and space–traditionally identified by the Pentagon. Hospitals and other private and public infrastructure, like courts, do not have anti-missile defenses but they do need robust cyber security. Intending to scare government and corporate leaders into addressing the threat, the authors predict that the next major war will be provoked by a cyberattack (Clarke and Knake, 2019: 7). As described earlier, recent ransomware attacks on court systems demonstrate an awareness of the vulnerabilities and an interest in exploiting these vulnerabilities, whether for commercial or financial gain or for disrupting society, economy, and institutions.

In response to cyber threats, companies and universities are building cybersecurity training facilities that simulate cyberattacks and train staff how to detect and respond. "We can put malware that steal information from our network on it, and allow my team to go in and fix the situation–not in theory, but actually do it," said Ron Green, chief security officer at Mastercard (Janofsky, 2019b, B4).

**Box 4. Deepfakes**
Deepfakes, the term used to refer to counterfeit video, audio recordings, and photos created using a machine-learning technique called a "generative adversarial network" (GAN), are a way to algorithmically generate new types of data out of existing data sets. These forgeries have been successfully used to obtain money under false pretenses. For example, in at least three cases, fake "Chief Executive Officers" stole millions of dollars by convincing other employees to act (Waddell and Kingson, 2019). Deepfake audio and video can be created using artificial intelligence programs that learn how to replicate a person using their online digital footprint, such as audio and video recordings. Manipulation of images and videos using artificial intelligence readily could become a dangerous mass phenomenon because of the realism, the technology's ease of use, and the current lack of affordable, reliable countermeasures. In June 2019, a video of Facebook CEO Mark Zuckerberg giving a talk was posted on Instagram; it was a fake. A Chinese-made app, Zao, that uses deepfake technology became the most downloaded free app after it was launched on August 30, 2019. It uses deepfake technology, including artificial

intelligence, to produce videos, audio recordings, and photos that are very realistic forgeries. While the backlash over Zao is focused on data privacy and identity theft, the free app raises increasing concern about the security risks it and similar deepfakes pose (Li, 2019: A8).

Another area for concern in cyberspace is the Internet of Things (IoT). The Federal Trade Commission (FTC) defines the IoT as "devices or sensors–other than computers, smartphones, or tablets–that connect, store, or transmit information with or between each other via the Internet" (FTC, 2015). By 2020, the FTC estimates that there will be 50 billion connected devices worldwide, including health and fitness wearables, connected cars, home-security devices, and digital assistants. These devices are a gateway to a treasure trove of personal, home, and business data. The benefits of their use are numerous, including real-time health monitoring, energy conservation, and time savings, but the risks of data misuse, including the compromise of safety and other systems from hacking, are at least as numerous. John Moor, managing director of the IoT Security Foundation stated: "Your insecure product may not be the ultimate target but could provide the pivot point for an attack elsewhere in the system" (IoT Security Foundation, 2015). As these devices and the broader landscape of connected computers and systems evolve, governments and the private sector have struggled to effectively identify, protect, and recover vulnerable networks, systems, functions, and data (White House, 2018b).

The breadth of cybersecurity threats cannot be overstated. The National Institute of Standards and Technology (NIST), in its *Framework for Improving Critical Infrastructure Cybersecurity,* reminds us that the "national and economic security of the United States depends on the reliable functioning of critical infrastructure" (NIST, 2014). While the information technology and industrial control systems support critical infrastructure services, they have diversified and evolved without enough protection, increasing the vulnerabilities of the nation's critical infrastructure (NIST, 2018).

## Other Threats

Although the focus of this article is primarily on the CBRNE and cyber threats, there are other threats that must be considered in a WGA. A horrible example was the absence of a WGA in a response to the 1986 nuclear-power-plant explosion and radioactivity leak in Chernobyl in Ukraine, which was a part of the then Soviet Union. The Chernobyl accident was a manmade disaster that resulted in a loss of life, a long-term public health crisis, and a human-exclusion zone of 1,600 square miles. Russian authorities first dismissed the disaster as a relatively minor industrial accident, failed to identify the magnitude of the disaster, kept it a closely held secret from its own people and the international community, minimized the planetary peril of the disaster, and for a long time rejected scientific and international cooperation in dealing with the disaster (*Encyclopedia Britannica,* 2019).

Climate change is causing environmental upheaval such as the droughts, heat waves, and floods around the world, which in turn are having destabilizing effects on societies. For example, in the Sahel countries of Africa south of the Sahara, droughts and floods have destabilized regions and caused civil wars as people fight over fertile land (*Economist*, 2019c, d). Droughts in Guatemala, Honduras, and El Salvador similarly have destabilized that region (Frey, 2018; *see also,* Global Disaster Alert and Coordination System). The threats of natural disasters, pandemics, bioterrorism, and chemical and nuclear attacks demand a coordinated rapid response by many actors from dozens of governmental and nongovernmental entities.

# Ideological, Theoretical, and Practical Barriers Facing the WGA in the Third Branch

Judiciaries' resistance to novelty is deeply rooted in law and practice. By design and for various reasons, United States courts tend to shy from innovation, adopting new technologies often decades after these technologies have slipped into the mainstream of society. Courts are not designed to act in haste but in contemplation and thought. They are conservative; they rely on precedent; they prefer the tried over the untried. This design is enshrined in the *de jure* "law on the books" in states and nations. Judges and courts accordingly act deliberatively in practice.

## Judicial Independence, Separation of Powers, Checks and Balances, and Stare Decisis

The drafters of the U.S. Constitution, influenced by theorists such as the English philosopher John Locke and the French judge and political philosopher Montesquieu, as well as their own experiences in the American Revolution, provided for the separation and diffusion of powers among the executive, legislative, and judicial branches of government in Articles I, II, and III of the Constitution. The three branches were to be considered coequal, each a check and balance on the others. The resulting structures and the relationships among the units of government–notably, the allocation of powers among the three branches of government–present issues for a WGA to confront. The structures and relationships were designed neither for expedition nor always for coordination–sometimes, not even for cooperation.

## Theoretical Difficulties

Three related concepts–the independence of the judiciary, the separation of powers, and the structure of checks and balances–may be inconsistent with the WGA. Notable among the difficulties are the interrelated doctrines of the independence of the judiciary and the separation of powers of the judicial, legislative, and executive branches, both of which doctrines are fundamental to democratic governance. The separation of powers provides a system of shared power known as checks and balances. Judicial independence secures for individual judges, courts, and court systems the independence and, thus, the impartiality to resolve disputes according to the laws of the Constitution and those passed by the legislative branch and to shield the third branch from any improper influence from the other branches of government or private or partisan interests. By design, this separation and sharing of power, and checks and balances, make democratic governance inefficient and indeed antithetical to a rapid response, "one-stop government" demanded of the WGA.

Another doctrine in the United States' legal system that contributes to inefficiencies and runs counter to a WGA is *stare decisis,* a precedent-honoring approach through which a court maintains the status quo, reaffirming a previous decision or basing a new decision on its own prior decisions for the purpose of maintaining continuity and reliability.

## Practical Barriers: The Law in Practice

Arguably, the safeguards of judicial independence and separation of powers constitute a serious impediment to WGA. The same can be said about the law in practice.

Buoyed by theory and tradition, judicial independence has particularly served as a rallying cry for reform, especially for state-court judges, since the 1950s.[3] Judges in the United States understandably chafe at real and perceived threats to their independence, be those threats from members of the executive and legislative branches or from their partisans. Often, the members of the other two branches seek to dictate and demand the kind of agility and flexibility, and joint action, that is an integral part of a WGA, not only in the decision-making process of the courts but also in areas of court operations, administration, and governance.

In practice, in the name of judicial independence, judges resist being absorbed or managed by the other two branches (Tobin, 1999: 15). They have sought to ward off the intrusion of the officials of the other branches; to eliminate political considerations in the selection, tenure, and salary of judges; to build what others determine to be more coherent court structures and governance if such may tamper with court organization and jurisdiction to suit political needs; to bring lawyers under the control of courts rather than the other way around; to have the authority against the legislative branch to prescribe rules of practice and procedure in the courts, civil, criminal, and evidentiary; to have greater control of their budgets and better access to resources; and to assert that the judicial branch has the inherent authority to order the other branches to supply the resources necessary to perform their functions. Their message to the other branches is clear: Give us the requisite resources for which we are dependent on the executive and legislative branches, and then leave us our independence to handle the duties of the third branch.

Not surprisingly, the judicial actions noted above have not endeared judges and courts to officials of the other branches. Relations between the judiciary and the other branches often have been tense and fraught with distrust, which has raised practical barriers to WGA. "Some legislators complain that the judiciary is too remote and self-absorbed and not really accountable to anyone," wrote the late Robert Tobin of the National Center for State Courts (1999: 16).

Nonetheless, justice systems are beginning to pay greater attention to the security and safety threats to society (a favorable development to courts' participation in a WGA that we will mention in the next section). Most judicial officials today do not register much alarm and urgency about threats beyond the courthouse walls–even those that impact or will impact the operation of those courthouses.

Just as every other component of a democratic government needs to be mobilized for a WGA to succeed, justice and law professionals will remain critical to ensuring the rule of law and the application of justice. However, with the exception of general references to the rule of law, the strengthening of governance, and improvement of information sharing to target criminal activity in such WGA-related references as the National Security Strategy 2017 (White House, 2017b: 51; see also Ellis, 2019: 35), justice systems' participation in WGA, as defined, is conspicuously absent from serious discussions today.

In turn, WGA generally is absent from the writings in the field of court administration. Though "courthouse security" has been of utmost concern in judicial minds, it generally does not reach beyond the courthouse walls (Rogers, 2019). As we suggested earlier, this state of affairs reflects an inward-looking focus that Tobin characterized as remote and self-absorbed.

Alexander B. Aikman, in his 2007 book, *The Art and Practice of Court Administration*, describes court administration's external relationships, defined as exclusive of the court administration's relationships with the judges and their staffs and with the litigants and their attorneys. He identifies the following groups as important: 1) members of the general public using the court but who are not involved in litigation; 2) local colleges and universities regarding volunteers and internship programs; 3) local victims-rights and advocacy groups; 4) court watchdog groups; 5) local school officials and teachers regarding student education programs, including peer courts and court tour programs; 6) community-service programs; 7)

public and private volunteer coordinating programs; 8) credit-reporting and other investigative groups; 9) academic and other researchers; and 10) local media (Aikman, 2017: 310-11). What seems most important about the courts' relationships with these is their potential contribution to the improvement of the courts' *internal* operations.

The situation may be changing. A trend favorable to judicial systems' participation in a WGA can be ascertained in several developments over the last decade, and arguments can be raised that support such a trend. We briefly discuss this trend in the next two sections.

# Trends Favoring WGA Participation by Courts

## Recent Developments

Among recent developments favorable to justice systems' active participation in a WGA are the courts' increased public engagement; their disaster-recovery and business-continuity preparedness since the al-Qaeda attacks on September 11, 2001; pandemic preparedness; and United States federal and state litigation resulting in judicial opinions related to emergency preparedness, response, and recovery.

*Increased Public Engagement.* The Public Engagement Pilot Initiative is a collaboration of the National Center for State Courts (NCSC) and the University of Nebraska Public Policy Center (National Center for State Courts, 2018). Six court systems in the United States are participating in the project, which aims to identify proven ways to build trust and confidence in the courts. Each of six pilot courts is working on a different aspect of court services in connection with public engagement. The Massachusetts Trial Court is recruiting leaders willing to "commit to a longer-term partnership" between the courts and the community. In Nebraska, the state supreme court wants to better recognize the needs of Native Americans. The Franklin (Ohio) Municipal Court is learning how underserved populations perceive specialized dockets and its Self-Help Resource Center. The Kansas City (Missouri) Municipal Court is integrating court user surveys into its public-engagement process. The Puerto Rico Judicial Branch is focusing on helping communities address neighborhood conflict. Finally, the Texas Office of Court Administration is building on results from its prior "Beyond the Bench" effort.

The chair of the pilot initiative, Chief Judge Anna Blackburne-Rigsby of the District of Columbia Court of Appeals, said that courts have been working for decades to improve public trust and confidence, but that, sadly, little progress has been made. She observed that the primary method courts have used is outreach to communities, but such an approach is limited. "Outreach is one-way communication," she said. "Engagement is different. It involves listening. It's a two-way."

*Disaster Preparedness.* In past disasters, state and local public-health practitioners and emergency responders treated courts not as a part of an independent branch of government but like they did other local or state executive agencies. As a result, for the most part, the judiciary was overlooked as an agent of a WGA. As noted by the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA), this changed in large part after the al-Qaeda attacks on September 11, 2001 and Hurricane Katrina in 2005 as state court and justice system officials focused their attention on court disaster recovery and business continuity (CCJ/COSCA Pandemic and Emergency Response Task Force, 2016).

Though the focus remained squarely on operational disruptions, a broader view of the threats to society as a whole was emerging. In 2006 COSCA recognized that the need for "comprehensive governmental coordination" was never more evident than it was immediately following Hurricane Katrina, demonstrating that "emergency planning requires an enormous amount of advance coordination among different court levels and between the courts and a host of state and local agencies on a wide range of facility, security, law enforcement and emergency management issues" (CCJ/COSCA, 2016).

Judge Robert P. Ringland of the 12th District Court of Appeals of Ohio has written a guide to prepare judges, court personnel, and members of the bar to address pandemics and other catastrophes that may occur and interrupt the administration of justice and the courts (Ringland, 2019). Although his focus is on the legal provisions and authorities for government emergency actions, and on operating the judicial system during a public health emergency, he conveys a clear sense of urgency about the threats of pandemics and other catastrophes to society as whole beyond the courthouse walls.

The Kosovo example of court data loss and its impact on the courts' continuity of operations and on society underscores the importance of courts as a critical infrastructure in a WGA in response to serious threats to the safety and security of nations. The United States Presidential Policy Directive, Critical Infrastructure Security and Resilience (PPD-21) acknowledges that essential services are critical underpinnings of American society (White House, 2013). Fostering resilience in government instills confidence in the public, itself key to productive recovery. PPD-21 establishes policy for the security and resilience of critical infrastructure against physical and cyber threats. As the coordinating federal agency, the Department of Homeland Security (DHS, n.d.) identified, and continues to address, 16 critical sectors—one of which is the Government Facilities Sector encompassing courthouses and office buildings that house critical equipment, systems, networks, and functions.

**Box 5. Courts Have Not Prepared for a Potential Pandemic**

Quarantine laws and statutes in many states have not been updated or tested since the influenza outbreak of 1918, which killed more than 675,000 Americans (CDC, 2018a), and for that and other reasons the courts are

not prepared to address a potential pandemic. As one example, on October 30, 2014, Chief Judge of the Maine District Courts Charles LaVerdiere received a call that the state had filed a petition to quarantine a nurse returning from Ebola-stricken West Africa who had planned to attend a large social function that evening. Chief Judge LaVerdiere needed to decide quickly whether to allow the nurse's quarantine. He determined that Maine had not met its burden of proof and denied the quarantine although it did require cooperation with monitoring and placed limits on her travel. A lot of "what ifs" went unanswered, underlining the need for pandemic-planning efforts.

"I was forced to make a life-or-death decision immediately. No decision was, in fact, a decision with potentially deadly consequences," LaVerdiere told the National Pandemic Summit in May 2019 at the University of Nebraska Medical Center in Omaha, home to the country's biocontainment unit where three Ebola patients were treated in 2014 (National Center for State Courts, 2019) . The summit brought together court leaders, public-health officials, legislators, and executive-branch officials to start a collective conversation about many potential legal issues concerning how states need to plan and prepare for a pandemic, which often not only includes quarantines of individual members of the public, as was the case in Maine, but also implicates the operations of courts, jails, prisons, and hospitals. Twenty-five states and three territories sent teams.

Defending against cybersecurity threats requires different technical and policy approaches than pandemics and natural disasters or biological and chemical terrorist attacks, which, for this analysis, are not completely unlike pandemics for planning and preparation. While the National Cyber Strategy of the United States of America (White House, 2018b) and Executive Order 13800 (White House, 2017a), among others, provide policy guidelines, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity provides industry standards and best practices for cybersecurity risk management for critical infrastructure (NIST, 2018). State, local, tribal, and territorial entities can also refer to the Government Facilities Sector Specific Plan of 2015 for strategic goals, objectives, actions, and priorities for enhancing security and resilience (DHS and GSA, 2015). By leveraging existing strategic guidance and employing a WGA for preparedness, response, and recovery, courts should be able to maximize personnel, funding, and equipment resources to enhance the physical and cybersecurity posture.

*Increasing Litigation Related to Emergency Preparedness, Response, and Recovery.* In a recent study, researchers at the Johns Hopkins Bloomberg School of Public Health and the Centers for Disease Control and Prevention (CDC) analyzed litigation related to emergency preparedness, response, and recovery activities from the September 11, 2001 terrorist attacks to December 31, 2015 (McCourt, Sunshine, and Rutkow, 2019). They identified 215 United States federal and state cases of actual or perceived mental, physical, or financial harm to individuals. Most of the cases stemmed from preparedness, response, and recovery activities related to hurricanes (57.7 percent) and terrorist attacks (16.7 percent). The most prevalent emergency-response activities at issue were disaster mitigation (29.3 percent), disaster clean-up (21.9 percent), a defendant's duty to plan (14.4 percent), evacuation (12.6 percent), and conditions of incarceration (12.1 percent).

The major function of courts is dispute resolution and the fact that these cases arose in the wake of major disasters is nothing new. The courts' mission is to respond to cases and controversies brought to them. Thus, they are reactive, not proactive. However, the scope of this litigation serves to raise awareness and a sense of urgency for a WGA that may increase its receptivity among judicial leaders.[4]

## Arguments in Favor of Third-Branch Participation in WGA

In addition to the concrete developments over the last decade that have contributed to increased receptivity to judicial systems' participation in WGA, there are several arguments that can be made. Perhaps most cogent is an emphasis of the principle of comity in governmental relations and the argument that the separation of powers is not absolute. Others, only briefly mentioned here, include the contention that the separation of powers was never intended to be absolute; that emergencies require emergency measures; and, finally, that the "whole" in "Whole-of-Government" means everyone.

*The Principle of Comity.* Judicial independence does not mean absolute autonomy or isolation. The five standards in the performance area of independence and accountability in the seminal *Trial Court Performance Standards,* or TCPS (Commission on Trial Court Performance Standards, 1997), combine the principles of separation of powers and judicial independence with the need not only for public accountability, but also for comity. *Black's Law Dictionary* (5th ed. 1979: 242) defines "comity" as courtesy, complaisance, respect, and a willingness to grant a privilege, not as a matter of right or obligation, but out of deference and goodwill. The TCPS takes the doctrine of comity beyond the legal sphere and into judicial administration, i.e., the practices, procedures, and organizational structures concerning the management of the administrative systems of the courts.

Standard 4.1 of the TCPS, "Independence and Comity," states: "A trial court maintains its institutional integrity and observes the principle of comity in its governmental relations," suggesting that comity is integral to public accountability. The commentary of the standard states:

For a trial court to persist in both its role as preserver of legal norms and as part of a separate branch of government, it must develop and maintain its distinctive and independent status. It also must be conscious of its legal and administrative boundaries and vigilant in protecting them. Effective trial courts resist being absorbed or managed by the other branches of government.… Effective court management enhances independent decision making by trial judges.… The court must achieve independent status, however, without damaging the reciprocal relationships that it maintains with others. Trial courts are necessarily dependent upon the cooperation of other components of the justice system over which they have little or no direct authority.

The link of judicial independence with public accountability is widely recognized, comity being an essential component. Indeed, accountability is a necessary condition of judicial independence and the separation of powers. This linkage recognizes that the greater degree of freedom from interference traditionally and necessarily enjoyed by the judiciary and courts compared to other public institutions (at least in much of the western world) must be balanced by the quid pro quo of transparency and accountability. While the TCPS has been influential in linking judicial independence and accountability, its incorporation of comity as an element of public accountability seems not to have been widely embraced.

Making comity in government relations a requisite of judicial independence and accountability is an imperative. Faced with far-reaching threats and rapidly developing problems, governments and the public itself can ill afford to insulate judiciaries from society, allowing them to be out of touch with rapid responses to various threats and problems, and isolated, insufficiently accountable to anyone. The principle and practice of comity by judicial actors opens the door for breaking the silo mentality and making the judicial branch amenable to a WGA.

Judges, court administrators, and other actors in the justice system should recognize the risks of not doing so. The doctrines and the terms used to describe judicial independence and the separation of powers may be construed by some observers as incompatible with–even antagonistic to–strategies of communication, coordination, and cooperation of the WGA. Such a view sets the judiciary in a precarious silo operating in isolation from other branches of government. The European Networks of Councils of the Judiciary (ENCJ), an organization of national councils of the judiciaries in the member states of the European Union (EU), recognized the risks of such a silo mentality, noting in its 2017 report on independence and accountability that a judiciary that “does not want to be accountable to society and has no eye for societal needs will not gain the trust of society and will endanger its independence in the short or long run” (ENCJ, 2017: 10), thus echoing Tobin’s criticism of the judiciary as “isolated and self-absorbed.”

*Separation of Powers Is Not Absolute.* The separation of powers of the three branches of government was not intended to be absolute in the sense of isolation. Rather, the separation of powers was intended by the authors of the United States Constitution to be for the purpose of judicial independence from the political and partisan executive and legislative branches. Indeed, the preeminent constitutional scholar Gerald Gunther argued that “political accommodations have predominated” and that this ambiguity may well have helped to combat the excessive concentration of powers in one branch of government (Gunther, 1980: 384).

That the separation of powers recognizes the need for political accommodations is evidenced by the process through which the National Environmental Policy Act (NEPA) has developed since its passage in 1969.[5] NEPA requires all federal agencies to include consideration of the environment in their decision making through the process of environmental impact statements (EIS) and, significantly, to involve the public before proceeding with any major federal action significantly affecting the human environment. To this end, it created the Council on Environmental Quality (CEQ) with responsibility for coordinating the EIS process and assisting federal agencies with NEPA compliance. The CEQ issued guidelines, memoranda, and eventually regulations to implement NEPA through executive orders because NEPA did not specify that the CEQ had the authority to issue rules or regulations to implement the law and did not give the CEQ enforcement authority.[6] NEPA also does not include a provision for judicial review or any standard of review by courts. Yet, courts, in conjunction with the CEQ, have played a significant and defining role in the implementation and interpretation of NEPA (Stevens, 1974).

In discussions of the WGA, the interpretation and implementation of NEPA by the CEQ within the Executive Office of the President, and the courts, illustrates that the separation of power is not absolute. Given the absence of CEQ authority to enforce compliance with NEPA, the courts became the refuge of environmental groups seeking to ensure that federal agencies complied with NEPA requirements. This process began in the first few years of NEPA implementation and has been critical to the interpretation and application of the law ever since. “[W]ithout ever appearing on the surface of the Guidelines, this relationship between the CEQ and the courts has been an intimate part of the process of NEPA’s growth,” wrote Daniel Mandelker and his colleagues. “Whether NEPA drafters contemplated judicial review of impact statements is not clear; the question was barely discussed in the legislative history. Judicial review has now become an integral part of the statute’s administration. It provides external rather than internal pressure for modifications in agency practice to comply with NEPA’s mandates” (Mandelker et al., 2018).

*Emergencies Require Emergency Measures.* Courts are not unfamiliar with expedited proceedings in appropriate cases when the constraints of time and urgency dictate that emergency measures be taken. Courts in all likelihood may need to set aside their usual practice to participate in a WGA in response to terrorist attacks and other extreme and unique threats. It is hard to imagine that courts would permit operational omissions or failures that increase threats to the security and safety of the public, albeit responding in a manner consistent with the provision of constitutional rights, notably due process.

*"Whole" Means Everyone.* The third argument in favor of justice systems' participation in a WGA is a simple one. Today's threats and risks demand coordinated and rapid responses by many actors in and out of government, judicial and administrative components of the third branch not excepted. There is a known-unknown matrix, and justice-system actors as likely as anyone else may be able to recognize something that might stave off a catastrophe, thwart a threat, or mitigate damage. It is far better for the judicial branch to be prepared for a WGA and not be needed than to be needed and be woefully unprepared, or, in other words, it is far better for the third branch to be a participant in a WGA than a bystander to a catastrophic occurrence.

# A Call to Action for Courts

The breadth, severity, and urgency of 21st-century threats facing us deserve the attention of courts and their justice partners, not just to mitigate the risks to the continuity of their operations, but to protect the safety and security of society as a whole. Criminals and terrorists take advantage of the political, social, and economic chaos following a catastrophe, whether it is naturally occurring, accidental, or deliberate. A WGA is needed to counter such threats to our public health, safety, security, way of life, and democratic values.

Since the al-Qaeda attacks on September 11, 2001, the anthrax letters the following week, Hurricane Katrina in 2005, and other incidents, courts have recognized the need for urgent actions in response to natural disasters and pandemics that threaten their "business continuity." However, the broader view of the threats shows that "emergency planning requires an enormous amount of advance coordination among different court levels and between the courts and a host of state and local agencies on a wide range of facility, security, law enforcement and emergency management issues" (CCJ/COSCA, 2016). Litigation stemming from preparedness, response, and recovery activities serves to raise awareness and a sense of urgency for a WGA involving judicial leaders. A narrow mindset and inward perspective are inadequate, shortsighted, and potentially dangerous as evidenced by the urgent decision making required for quarantine enforcement.

Several encouraging trends favorable to judicial systems' participation in a WGA can be ascertained in developments over the last decade: a growing body of judicial opinions related to emergency preparedness, response, and recovery since the 9/11 attacks; an increasing number of discussions within the judicial community; the National Pandemic Summit that included court leaders, public-health officials, legislators, and executive-branch officials; Judge Robert P. Ringland's *Public Health Preparedness Bench Book;* and the Public Health Law Program (PHLP), which is working "to improve the health of the public by developing law-related tools and providing legal technical assistance to public health practitioners and policy makers in state, tribal, local, and territorial (STLT) jurisdictions" (CDC, 2018b).

The ideological and theoretical arguments against and posited practical constraints of active participation in a WGA to the serious threats identified in this article do not bear close scrutiny. While judicial-branch representatives at the federal and state levels will not be among the first emergency responders, unlike the fire, police, and public-health workers, at the least, it is their obligation to participate in planning and preparedness. Courts are tradition-and precedent-bound institutions, and there is a critical stability for our republican democracy that comes with that status for justice to continue. But traditional thinking about the propriety of roles can become ossified and dangerous. The public's trust in the legitimacy and the relevance of courts are at risk if courts do not participate as members of a WGA. Michael Buenger, executive vice president and chief of operations of the National Center for State Courts, recently warned about the dangers of traditions and traditional thinking about courts at a meeting of the American Bar Association: "We can, if we are not careful, tradition ourselves into irrelevancy, constitutional words notwithstanding" (Buenger, 2019).

Based on our combined research for this article, as well as our own collective knowledge and experience across different fields, we are in unanimous agreement in drawing this conclusion: For the security and safety of the users and employees of courthouses, for the communities they serve, and for society as a whole, the leaders and managers of national and subnational justice systems must become active participants in a WGA in response to the risks and threats we identified.

As we were shockingly reminded by two of the most recent deadly mass shootings–one in Dayton, Ohio, and one in El Paso, Texas–we now face a new homegrown national security threat, one the United States Department of Justice (DOJ) has begun declaring to be "domestic terrorism."[7] "We use the term 'domestic terrorism' to refer to a broader array of threats ranging from anarchists extremism to different kinds of racially motivated violent extremism to different types kinds of environmental extremism," FBI Director Christopher A. Wray told Congress this summer (Calfas, Tau, and Elinson, 2019: A6; Federal Bureau of Investigation, 2019).

Spotting and stopping shooters in incidents of domestic terrorism like those in Dayton and El Paso is especially hard due to the legitimate constraints on law enforcement by the first (free speech) and second amendments (right to bear arms) of the United States Constitution. However, courts should not be rendered helpless; they cannot do nothing. In response to the security threats of domestic terrorism, for example, they should consider engaging with a WGA in future scenario planning, which originated in the armed forces during the Second World War and was widely adopted after the terrorist attacks of September 11, 2001. It is the process of mapping out several futures, planning how to respond to them, and possibly identifying telltale signs that may help in spotting and stopping domestic terrorism. The exercise could surface contributions of courts to a WGA response such as states' full participation in the National Instant Criminal Background Check System

(NICS)–state participation today is voluntary–and clarifying when it is lawful under privacy laws such as the Health Insurance Portability and Accountability (HIPPA) and the Family Educational Rights and Privacy Act (FERPA), to share records that may help spot potential threats.

Similar scenario-planning can focus on the other security and safety risks and threats discussed in this article. In a recent "leader" article and its corresponding annual set of speculative scenarios, "The World If," the *Economist* lauds scenario planning as shifting our perspective from the present and increasing our understanding of what may be possible in the future (*Economist*, 2019e: 12; *Economist,* 2019f).

There are, of course, always risks to embracing something new. But we believe that benefits accrue to the court leaders, managers, and courts willing to explore and engage with a WGA. Rewards come to the leaders and managers of organizations who favor the future over the past, who focus on opportunities, and who embrace innovation.

---

## ABOUT THE AUTHORS

**Ingo Keilitz, Ph.D.**, is former vice president of the National Center for State Courts, principal of CourtMetrics, and visiting scholar of the Public Policy Program at the College of William & Mary (W&M), and research associate of W&M's Global Research Institute.

**Katharine Jennings, Ph.D.**, is principal microbiologist and manager at Noblis, Inc., a nonprofit science, technology, and strategy organization working in the public sector.

**Susan A. Ehrlich, J.D., LL.M.** (biotechnology and genomics), is judge (ret.) of the Arizona Court of Appeals and a former member of the National Science Advisory Board for Biosecurity.

**Caroline N. Broun, J.D., M.S.** (fisheries and wildlife), is a lecturer, Ohio State University, former environment officer, United States Mission to the United Nations and United States Mission to the European Union.

**Kathryn H. Floyd, Ph.D.**, is director, William & Mary Whole of Government Center of Excellence and former Mass Violence and Terrorism Visiting Fellow, U.S. Department of Justice.

**Michael L. Buenger, J.D., LL.M**. (public international law), is executive vice-president and chief operating officer, National Center for State Courts, and former state court administrator for the states of Ohio, Missouri, and South Dakota.

---

## REFERENCES

- Aikman, Alexander B. (2007). *The Art and Practice of Court Administration.* Boca Raton, FL: CRS Press.
- Albert, Eleanor (2019). "North Korea's Military Capabilities." Backgrounder, Council on Foreign Relations, July 25.
- Assistant Secretary for Preparedness and Response (ASPR) (2019). *National Health Security Strategy 2019-2022*.
- Barnard, Anne, and Michael R. Gordon (2017). "Worst Chemical Attack in Years in Syria; U.S. Blames Assad." *New York Times*, April 4.
- Bauer, Shane (2019). "Fueling the Conflict." *Mother Jones,* May-June.
- British Broadcasting Corporation (1998). "So What Is Joined-up Government?" *BBC News*, November 23.
- Buenger, Michael L. (2019). "Rethinking the Delivery of Justice in a Self-Service Society." Speech. Spring meeting of American Bar Association, April 10, Minneapolis.
- Calfas, Jennifer, Bryon Tau, and Zusha Elinson (2019). "FBI Probes Ohio Shooter's Motives Citing Links to 'Violent Ideologies.'" *Wall Street Journal*, August 7.
- Calvert, Scott, and Jon Kamp (2019). "U.S. Cities Face Growing Cyberattack Risk." *Wall Street Journal*, June 8-9.
- Carlin, John P. (2016). "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats." 7 *Harvard Law School National Security Journal* 391.
- Centers for Disease Control and Prevention (CDC) (2018a). "History of 1918 Flu Pandemic." Pandemic Resources.
- — (2018b). "About Us." Public Health Professionals Gateway, Public Health Law.
- — (2019a). "2014-2016 Ebola Outbreak in West Africa." Viral Hemorrhagic Fevers.
- — (2019b). "Measles Cases and Outbreaks January 1-July 18, 2019."
- Christopher, George W., Daniel M. Gerstein, Edward M. Eitzen, and James W. Martin (2018). "Historical Overview: From Poisoned Darts to Pan-Hazard Preparedness. In J. Bouze, C. K. Cote, and P. J. Glass (eds.), *Medical Aspects*

*of Biological Warfare*. Fort Sam Houston, TX: Office of the Surgeon General, Borden Institute, United States Army Medical Department Center and School, Health Readiness Center of Excellence.

- Clarke, Richard A., and Robert K. Knake (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* New York, Penguin Press.
- Coats, Daniel R. (2019). *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Senate Select Committee on Intelligence, 116th Congress.
- Commission on Trial Court Performance Standards (1997). *Trial Court Performance Standards with Commentary.* Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice.
- Conference of Chief Justices (CCJ) and Conference of State Court Administrators (COSCA) Pandemic and Emergency Response Task Force (2016). *Preparing for a Pandemic: An Emergency Response Benchbook and Operational Guidebook for State Court Judges and Administrators*. Williamsburg, VA: National Center for State Courts.
- Crosby, Alfred W. (1972). *The Columbian Exchange: Biological and Cultural Consequences of 1492*. Westport, CT: Greenwood Publishing Group.
- Department of Homeland Security (DHS) (n.d.). "Critical Infrastructure Sectors." CISA Cyber + Infrastructure, Critical Infrastructure. Accessed July 12, 2019.
- Department of Homeland Security and General Services Administration (GSA) (2015). *Government Facilities Sector-Specific Plan: An Annex to the NIPP 2013*. Washington, DC: DHS and GSA.
- *Economist* (2019a). "Redesigning Life: The Promise and Perils of Synthetic Biology." *The Economist*, April 6.
- — (2019b). "Synthetic Biology." Technology Quarterly Supplement. *The Economist*, April 6.
- — (2019c). "How Climate Change Can Fuel War." *The Economist,* May 25-31.
- — (2019d). "How to Think about Global Warning and War." *The Economist,* May 25-31.
- — (2019e). "Futurology: Navigating the Rapids." *The Economist,* July 6.
- — (2019f). "The World If: Annual Speculative Scenarios." *The Economist*, July 6.
- Ellis, R. Evan (2019). "The U.S. Military in Support of Strategic Objectives in Latin America and the Caribbean." 8:1 *PRISM* 26.
- *Encyclopedia Britannica* (2019). "Chernobyl Disaster: Nuclear Accident, Soviet Union, 1986."
- European Networks of Councils for the Judiciary (ENCJ) (2017). *Independence, Accountability and Quality of the Judiciary: Performance Indicators 2017*. Report, 2016-2017.
- Federal Bureau of Investigation (FBI) National Press Office (2019). "FBI Statement Regarding Shootings in El Paso and Dayton." Press release, August 4.
- Federal Trade Commission (FTC) (2015). "Internet of Things: Privacy and Security in a Connected World." *FTC Staff Report,* January.
- Frey, John Carlos (2018). "All We Have Here Is Poverty and Drought: How Climate Change Is Causing a Food Crisis That Is Driving Central Americans to the U.S. Border." *The Marshall Project,* February 19.
- Garamore, Jim (2017). "Trump Announces New Whole-of-Government National Security Strategy." News release, U.S. Department of Defense, December 18.
- Gunther, Gerald (1980). *Cases and Materials on Constitutional Law. Tenth Edition.* Mineola, NY: Foundation Press.
- Hawking, Stephen (2018). *Brief Answers to Big Questions.* New York, Bantam Books.
- Internet of Things (IoT) Security Foundation (2015). *Make it Safe to Connect: Establishing Principles for Internet of Things Security.* West Lothian, Scotland: IoT Security Foundation.
- Janofsky, Adam (2019a). "How to Haggle with Your Hacker." *Wall Street Journal*, August 26.
- — (2019b). "Companies Train Staff in Cybersecurity Using Hacking Simulators." *Wall Street Journal*, September 4.
- Koblentz, Gregory (2018). "The Synthesis of Horsepox Virus and the Failure of Dual-Use Research Oversight." *Pandora Report,* January 20.
- Li, Shan (2019). "Deepfake Chinese App Zao Faces Privacy Backlash." *Washington Post*, September 4.
- Lin, Herbert (2017). "Attribution of Malicious Cyber Incidents: From Soup to Nuts." *Journal of International* Affairs, March 9.
- Mandelker, Daniel R., Robert L. Glicksman, Arianne Michaelek Aughey, Donald McGillivray, and Meinhard Doelle (2018). *NEPA Law and Litigation*. Toronto, CN: Thomson Reuters Environmental Law Series.
- McCourt, Alexander D., Gregory Sunshine, and Lainie Rutkow (2019). "Judicial Opinions Arising from Emergency Preparedness, Response, and Recovery Activities." 17 *Health Security* 240.
- Murdoch, Jason (2019). "What Is Ransomware? Georgia Court System Falls Victim to Cyberattack as Towns and Cities in Florida Pay More than $1 Million to Hackers." Tech and Science, *Newsweek,* July 2.
- National Academies of Sciences, Engineering, and Medicine (2018). *Biodefense in the Age of Synthetic Biology*. Washington, DC: National Academies Press.

- National Center for State Courts (2018). "Moving the Needle on Public Trust in the Courts." *@ the Center*, August 18.
- — (2019). "Courts Can't Prepare Enough for a Potential Pandemic." *@ the Center*, May 30.
- National Institute of Standards and Technology (NIST) (2014). *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0*. February 12, Gaithersburg, Maryland.
- — (2018). *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1*. April 16, Gaithersburg, Maryland.
- National Nuclear Security Administration (2018). *Prevent, Counter, and Respond—A Strategic Plan to Reduce Global Nuclear Threats: Fiscal Year (FY) 2019-FY 2023.* Report to Congress. Washington, DC: National Nuclear Security Administration, U.S. Department of Energy.
- National Science Advisory Board for Biosecurity (NSABB) (2006). *Addressing Biosecurity Concerns Related to the Synthesis of Select Agen*ts. December.
- — (2007). *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information*. June.
- Noyce, Ryan S., Seth Lederman, and David H. Evans (2018). "Construction of an Infectious Horsepox Virus Vaccine from Chemically Synthesized DNA Fragments." *PLOS One,* January 19.
- Osterholm, Michael T., and Mark Olshaker (2017). *Deadliest Enemy: Our War Against Killer Germs.* New York: Little, Brown and Company.
- Pickart, Francoise (2018). "The 2018 NYC Public Health Risk Assessment." Presentation, NYC Health.
- Realuyo, Celina B. (2019). "The New Opium War: A National Emergency." 8:1 *PRISM* 132.
- Richards, Dennis, and David Kavanagh (2001). "Departmentalism and Joined-up Government: Back to the Future?" 54:1 *Parliamentary Affair*, January.
- Ringland, Robert P. (2019). *Public Health Preparedness Bench Book: A Guide for the Ohio Judiciary and Bar on Legal Preparedness for Public Health Emergencies and Routine Health Cases*. Supreme Court of Ohio.
- Rogers, Donna (2019). "Courthouse Security." *Courts Today,* June/July, p. 8.
- Shaw, Julie (2019). "Cyber Attack Cripples Philadelphia Court System Websites, Computer Programs." *Philadelphia Inquirer*, May 30, 2019.
- Stevens, Herbert F. (1974). "The Council on Environmental Quality's Guidelines and Their Influence on the National Environment Policy Act." 23 *Catholic University Law Review* 547.
- Terry, Madeleine, Maggie Dene, Molly Dinneen, and Colin Evert (2019). "We Cannot Do This Alone: Combating National Security Challenges with the William & Mary Whole of Government Center of Excellence." *Small Wars.*
- Tobin, Robert W. (1999). *Creating the Judicial Branch: The Unfinished Reform.* Williamsburg, VA: National Center for State Courts.
- Waddell, Kaveh, and Jennifer A. Kingson (2019). "The Coming Deepfakes Threat to Businesses." *Axios,* July 19.
- White, Nathan (2014). "Organizing for War: Overcoming Barriers to Whole-of-Government Strategy in the ISIL Campaign." *Small Wars*, December 28.
- White House (2013). Presidential Policy Directive (PPD-21)—Critical Infrastructure Security and Resilience. February 12.
- — (2017a). Executive Order 13,800 of May 11, 2017: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 82 *Federal Register* 22391.
- — (2017b). *National Security Strategy of the United States of America.* Washington, DC: White House.
- — (2018a). *National Biodefense Strategy*. Washington, DC: White House..
- — (2018b). *National Cyber Strategy of the United States of America*. Washington, DC: White House.
- — (2018c). *National Strategy for Countering Weapons of Mass Destruction Terrorism*. Washington, DC: White House.
- — (2019). *National Intelligence Strategy of the United States of America*. Washington, DC: Office of the Director of National Intelligence.
- World Health Organization (WHO) (2014). Statement on the First Meeting of the IHR Emergency Committee on the 2014 Ebola Outbreak in West Africa. August 8.
- — (2016a). *International Health Regulations Third Edition*. Geneva: World Health Organization.
- — (2016b). "Situation Report: Ebola Virus Disease." June 10.
- — (2019). "Ebola Outbreak in the Democratic Republic of the Congo Declared a Public Health Emergency of International Concern." News release, Geneva.

*All statements of fact, opinion, or analysis expressed are those of the authors and do not reflect the official positions or views of the United States Government or of any institution with which the authors may be associated. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or endorsement of the authors' views.

1. Personal communication, Pranvera Reçica-Kirkbride, acting chief of party, USAID/Millennium DPI Partners, Justice System Strengthening Program in Kosovo, August 20, 2019.
2. The outbreak of a disease that occurs over a wide geographic area and affects an exceptionally high proportion of the population.
3. Among the "long train of abuses and usurpations" leveled against King George III of Great Britain in the United States Declaration of Independence of July 1776 is: "He has made Judges dependent on his Will alone, for the tenure of their offices, and the amount and payment of their salaries."
4. Some may argue that this small sample of cases does not necessarily reflect a nexus between emergency preparedness, response, and recovery.
5. 42 USC §4321 et seq. (1969), as amended.
6. The absence of CEQ authority to draft rules and regulations, as well as to enforce NEPA, can be contrasted with the Environmental Protection Agency's authority to both draft regulations to implement environmental laws and to enforce those regulations.
7. A "mass killing" is one in which three or more people are killed in a single incident (Investigative Assistance for Violent Crimes Act of 2012, sec. 2(a)(2)(i), P.L. 112–265, 126 Stat. 2435 (2013); 6 U.S.C. §455(d)(2) ("the term 'mass killings' means 3 or more killings in a single incident"); 28 U.S.C. §530C(b)(1)(M)(i)(I) (same)).


## NATIONAL ASSOCIATION FOR COURT MANAGEMENT

The National Association for Court Management is a nonprofit organization dedicated to improving the quality of judicial administration at all levels of courts nationwide. In carrying out its purpose, the association strives to provide its members with professional education and to encourage the exchange of useful information among them; encourages the application of modern management techniques to courts; and, through the work of its committees, supports research and development in the field of court management, the independence of the judicial branch, and the impartial administration of the courts.



EDITOR
TASHA RUTH
Manager, Case Management Section, Supreme Court of Ohio
(614) 387-9414 courtmanager@nacmnet.org

MANAGING EDITOR
CHARLES CAMPBELL
National Center for State Courts
300 Newport Ave., Williamsburg, VA 23185
(757) 259-1838 ccampbell@ncsc.org