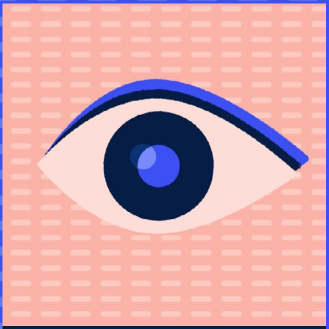
Digital Threats to Democracy: Glass Nations, Glass People

Alexa Wehsener, Technology for Global Security



FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security (T4GS) and the Center for a New American Security (CNAS) examines the elements and potential implications of digital threats to democracy over the next ten years. This post dives into the challenges complex fragile infrastructure could pose to democracy over the next ten years.

UNDERSTANDING FRAGILE COMPLEX INFRASTRUCTURE

Complex physical and societal infrastructures in democratic societies are becoming increasingly vulnerable. While physical infrastructure works to support the population, its design criteria is inherently a result of social planning processes. As advanced and powerful technologies rapidly diffuse, operating these tools often requires minimal resources and/or technical expertise. Therefore, a growing number of non-state actors, "hacktivists," and individuals can target digital-physical systems. Further, malign actors are increasingly exploiting the pre-existing social fractures within democracies by targeting populations and democratic institutions.

SOCIAL VULNERABILITY

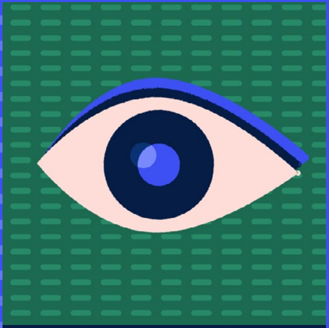
New technologies can enable and strengthen social resilience through localized support infrastructure and social connectedness. When new technologies are integrated into society, however, they can initially create structural weaknesses, since societal norms and standards for ensuring resilience have not yet been established. In addition, lack of education surrounding proper cyber hygiene contributes to weakened societal and physical resilience.

Democratic societies are increasingly vulnerable to attack and manipulation due to systemic weaknesses. Digital gray-zone threats take advantage of Western societies by further dividing and weakening government, industry, and civil society—precisely the institutions necessary to defend against these complex threats. Malign actors and political/private sector adversaries could capitalize on these vulnerabilities to worsen pre-existing tensions and exploit economic, political, racial, ethnic, and gender fault lines. Reality apathy, digitally impaired cognition, and weakened media institutions further contribute to a weakened societal resilience.

VULNERABILITY OF PHYSICAL INFRASTRUCTURE

Emerging technologies are increasing the interconnected nature of physical infrastructure. Critical infrastructure has been increasingly integrated with information and communication technologies, making key parts of society reliant on digital systems to operate. As a result, disruption or damage to one part of the system can rapidly spread to another—making complex infrastructure such as power plants, telecommunications, energy centers, and transportation systems attractive targets for malign actors.

The rapid proliferation of Internet of Things (IoT) devices further increases the vulnerability of various critical elements of public and private infrastructure. Put simply, more devices online equates to more potential pathways and targets for



FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security (T4GS) and the Center for a New American Security (CNAS) examines the elements and potential implications of digital threats to democracy over the next ten years. This post dives into the challenges complex fragile infrastructure could pose to democracy over the next ten years.

attacks. Several technical components of these new systems make them more effective facilitators of digital espionage and attacks:

— Lethal malware deployed in critical infrastructure with "killer code" enables the possibility of large-scale, fatal consequences in the physical world.
— Software-based 5G systems will be more vulnerable than prior networks because there are no choke points to shut off systems that are under attack. In the rush to 5G, nations still have not fully dealt with the vulnerabilities and weaknesses of 4G, or even earlier predecessors.
— The open architecture of mobile cloud computing makes it particularly vulnerable, as does the versatility of mobile terminals, providing multiple avenues through which attacks can be launched.

The speed at which technology is evolving enables complex cyber-attacks faster than the equivalent cybersecurity defenses can adjust—much less the appropriate or necessary policies—causing circular shifts in the digital offense-defense balance. Cyber-attacks can have physical impacts by taking out power grids, transportation systems, telecommunications, and digital systems—increasingly putting human lives directly at risk.

VULNERABLE NATIONS MAKE VULNERABLE SOCIETIES

Digital asymmetric warfare targets physical infrastructure as well as the population. It often involves difficulty attributing attacks that may be traced back to proxy groups operating on behalf of foreign governments. Potential effects to democracy could be a sense of loss of power and awareness for citizens, resulting in further diminishing the perception of democratic institutional legitimacy.

Telecommunications and supply chain infrastructure are both a physical and social vulnerability. A lack of resilient infrastructure within U.S. telecommunications systems could affect democracy by increasing reliance on external actors for the ability of the populace to communicate—a vulnerability for democracies built on the backbone of independence. As 5G security researchers Ahmad and Kumar write, "5G will connect critical infrastructure that will require more security to ensure safety of not only the critical infrastructure but safety of the society as a whole."

Democracies must cease pushing their vulnerabilities 'under the rug' and instead seek ways to incite systemic change that will strengthen social and physical infrastructure resilience.

Alexa Wehsener works as a research analyst at Technology for Global Security. Passionate about the broadening space in which emerging technologies are meeting the defense sector, Alexa focuses the majority of her work on the intersection of AI and US NC3, as well as the influence of emerging technologies and platforms on warfighting and democratic institutions.

CNAS | T4GS TECHNOLOGY FOR GLOBAL SECURITY