CYBERSECURITY

GETTY IMAGES

Culture Crashers

DHS remains vigilant amid growing digital foreign threats

By Matt Alderton

SINCE 2003, THE U.S. Department of Homeland Security (DHS) has dutifully executed its mission of protecting Americans from terrorist attacks on U.S. soil. Whether it can successfully safeguard the nation for another 20 years, however, depends on its ability to recognize threats that didn't exist when the department was conceived.

Increasingly, foreign adversaries are attacking America's tech-dependent economy and culture, spurring Congress to establish DHS' Cybersecurity and Infrastructure Security Agency (CISA) in 2018.

"DHS was formed before the iPhone was invented. Here we are 20 years later, and technology underpins so much of what we do," explains CISA Executive Director Brandon Wales. "This has created tremendous vulnerabilities."

Even as CISA fights cybersecurity risks like hacking and ransomware that can be levied against critical infrastructure, DHS must foresee inconspicuous attacks against less tangible targets — not the least of which is democracy itself, which U.S. adversaries seek to undermine by way of culture disruption.

"Hostile nation-states want to exploit weaknesses in the United States, and some of those weaknesses are cultural divides," Wales says. "Their goal is not to pick one side or the other. In many cases, it's to exploit and enhance divisions inside the American population."

Because it allows them to sow divisions with increased speed and scale,

CONTINUED »

technology is a key enabler. "They're exploiting technology ... that was designed to bring Americans together, and they're using it to divide us," Wales continues. "That is now part of the playbook of our adversaries, and we need to understand it so that we can do everything we can to protect against it."

WEAPONIZING POLARIZATION

Perhaps the best-known example of "culture disruption" is Russia's interference in the 2016 presidential election.

According to the Senate Select Committee on Intelligence, which investigated the matter, a Kremlin-backed troll farm known as the Internet Research Agency (IRA) attempted to sway the election by creating fake American personas on social media and using them to disseminate false information. While the IRA exploited election-related content, the committee found, its main focus was "exacerbating existing tensions on socially divisive issues."

At that time, Suzanne Spaulding was undersecretary for DHS' National Protection and Programs Directorate (NPPD), the department's cybersecurity arm prior to CISA. In the lead-up to the election, she says, NPPD focused heavily on securing voting machines, voter registration databases and other election infrastructure. It wasn't until after the election that it appreciated what the actual threat had been.

"If you think about elections in terms of functions instead of assets, the function we're trying to protect is the peaceful transition of power. For that to occur, the American public has to have confidence in the legitimacy of that process," notes Spaulding, now senior adviser for homeland security at the Center for Strategic and International Studies (CSIS), where she is director of the center's Defending Democratic Institutions project. "When you think about it that way, disinformation operations that are designed to undermine public confidence in our elections strike at the very heart of our democracy."

The same tactics that Russia used for election interference could be used to weaponize culture wars around issues such as abortion, LGBTQ+ rights, race, immigration, law enforcement or the Second Amendment.

"Information operations that are designed to exacerbate divisions and polarization in our society ... encourage us to create a sense of identity around grievance rather than shared aspirations and shared values," Spaulding says. "That weakens us as a nation because it makes it harder for us to come together to pursue our national interests."

"DHS was formed before the iPhone was invented. Here we are 20 years later, and technology underpins so much of what we do. This has created tremendous vulnerabilities."

– BRANDON WALES, executive director, CISA

ASSOCIATED PRESS

AI-generated images, created by British journalist Eliot Higgins, portray a fictional arrest of former President Donald Trump.

Even the most intangible threats can have real consequences, notes Spaulding, who cites the 2020 bombing outside an AT&T facility in Nashville, Tenn., the perpetrator of which had subscribed to conspiracy theories spread online — including beliefs that 5G networks accelerated the spread of COVID-19 and are a tool for government surveillance of citizens.

"These kinds of narratives are out there, and their impact is clearest where you've got potential for violence and attacks on critical infrastructure," Spaulding says.

DEEPFAKES RISING

"Culture disruption has been part of the way nations interfere with each other's business to accomplish their objectives going back millennia," explains former CISA official Bryan Ware, now chief development officer at cybersecurity company ZeroFox. "What's different now is the ability to use information technology to propagate and further those messages."

This is especially evident in the rise of deepfakes — fabricated yet convincing audio, images or videos that are generated using artificial intelligence (AI) and spread virally via social media.

Examples abound. In 2018, actor Jordan Peele produced a deepfake featuring President Barack Obama. In it, Obama appears to be delivering a public service announcement about disinformation. Midway through, however, a split screen reveals that the voice actually belongs to Peele, whose facial expressions and mouth movements are being transferred to Obama's likeness with the help of AI.

"What deepfakes can do, essentially, is disrupt truth," explains Rijul Gupta, founder and CEO of synthetic media platform DeepMedia AI. Deepfakes have gotten so good — they can even clone voices — that videos spreading falsehoods about vaccines, elections, climate change or U.S. military actions could have serious consequences, he says.

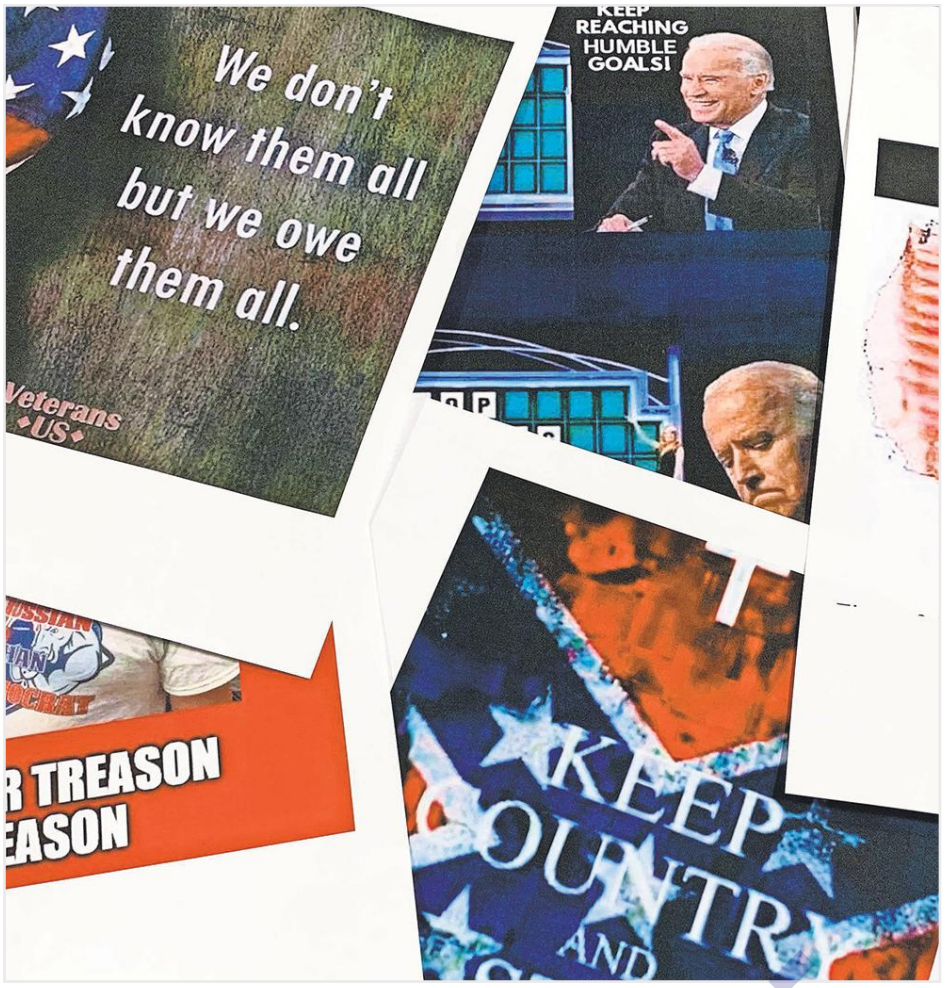
"What happens when the United States has to get involved in a situation that is absolutely critical to national security, but a large part of the population has stopped believing the truth?" Gupta asks. "You lose political support, which can impact even things like recruiting for the armed forces. It affects all parts of our society, from the government to the economy."

It's not just deepfakes of world leaders that could have consequences. It could be deepfakes of family, friends and neighbors — or individuals who don't even exist.

"It's classic counterintelligence: creating propaganda ... to make us fight each other instead of fighting a real enemy," Gupta continues. "It's possible right now to write a Python program that

CONTINUED »

CYBERSECURITY



ASSOCIATED PRESS

A Kremlin-backed troll farm's attempts to influence the 2016 presidential election represents the most glaring example of culture disruption in recent memory.

creates 10,000 identities with 10,000 unique voices. I could randomly generate statements that all sound different but say basically the same thing about how people on the left are talking bad about people on the right, or vice-versa. I could then generate videos and post them on social platforms. I could do all that in 24 hours."

FIGHTING FALSEHOODS

DHS in April 2022 announced the formation of a Disinformation Governance Board that would develop best practices for identifying and responding to false information deliberately spread by foreign governments and other adversaries.

Although DHS promised the board would operate with full transparency and with safeguards to protect civil liberties, objections from Republicans in Congress persuaded Secretary of Homeland Security Alejandro Mayorkas to dissolve the group just months after establishing it.

That was a mistake, says Richard Searle, vice president of confidential computing at data security firm Fortanix. "This technology is so complex in terms of its scope and impact that I think you need a holistic approach," Searle says. "The cancellation of that body within DHS was problematic because it could lead to fragmentation and duplication of effort."

Still, DHS says it remains well-equipped to mitigate the impact of information operations on its mission space.

Central to its efforts is DHS' Science and Technology Directorate (S&T), which conducts research and development on emerging technologies to understand threats and opportunities.

"S&T lives at an interesting point between trying to tap into what is emerging for the betterment of the nation while at the same time having to anticipate how it is likely to be misused," says S&T Chief Scientist Samuel Howerton. "That's a real challenge in this digital world that we live in today, because the threat evolves at a speed that the government has typically not been prepared for."

To keep pace with adversaries, S&T leverages both internal and external experts. "When something comes onto the scene more suddenly than we expected, we go and have conversations with the companies or researchers behind it to better understand the limits of the current technology and where they think it will go," says Howerton, who cites as an example generative AI, which made waves when OpenAI unveiled ChatGPT in November 2022.

To understand the impact of generative AI on homeland security, DHS in April established an Artificial Intelligence Task Force that will identify AI challenges and opportunities within DHS' mission set.

"We are at the very nascent stages of AI, and we don't fully understand yet how the threats to and from it will evolve," says CISA's Wales, who reiterates the importance of industry partnerships. He says his agency, for example, is actively working with AI companies to make sure that their intellectual property is safe from U.S. adversaries who may wish to steal it, that they design products with security baked into them and that they develop solutions to national security threats that may originate with their technology.

"It's classic counterintelligence: creating propaganda ... to make us fight each other instead of fighting a real enemy."

– RIJUL GUPTA, founder and CEO, DeepMedia AI

DeepMedia AI, for one, is doing its part by developing solutions for detecting deepfakes alongside platforms for generating them. Specifically, it's training machine-learning algorithms to automatically identify deepfakes by analyzing microfacial features for temporal inconsistencies — for example, eye and mouth movements from frame to frame in a video.

"If you have millions of fake faces and voices in your dataset, made with the latest and greatest synthetic face and voice algorithms, then you can develop machine-learning technology that can pinpoint reality from fiction," says Gupta, who favors regulations that would require action from tech companies — such as embedding detection tools in social media platforms or internet browsers to create public literacy around disinformation and associated culture disruption.

"Recently, the Chinese government developed regulations that forced social media platforms in China to detect and label deepfake content as synthetically manipulated," Gupta says. "I think that type of regulation can be adopted in the United States."

'DETERRENCE THROUGH RESILIENCE'

In societies that value freedom of speech and freedom of expression, disinformation is tricky business. Instead of trying to stop it outright, a more effective approach is building resilience against it, suggests DHS Assistant Secretary for Cyber, Infrastructure, Risk and Resilience Iranga Kahangama.

"Cybersecurity is not just fixing and patching things that are broken. Also, it's making sure pieces of critical infrastructure can persevere even while they're down," Kahangama says.

What's true of electric grids and water utilities — which are made resilient with manual backups that allow them to continue operating even if their digital controls are incapacitated — also is true of democratic institutions and social discourse.

"I think it's important to show ... our adversaries that we have perseverance through these issues as a matter of deterrence," Kahangama continues. "Deterrence through resilience is a concept we've learned from the Ukrainians, who have continued to operate in the course of very significant threats."

Resilience to disinformation and culture disruption starts with education. "We want citizens to ... recognize something that doesn't seem authentic or credible," Ware says. "That kind of recognition by individuals could be the best inoculation we have against these kinds of threats."

Spaulding agrees — which is why she helped CSIS launch its Civics at Work initiative, which engages with businesses to teach civics to its employees as a matter of national security.

"One of the key antidotes to efforts at undermining public trust in democracy is to teach democracy," Spaulding says. "How do you do that? You reinvigorate civics at all ages — in K-12, but also for adults. ... If we could reinstill in our population the notion of civic responsibility, that would go a long way toward building resilience against disinformation operations."