VIRTUAL THREATS

The Council on Foreign Relations' Adam Segal '90, PhD '00, is an expert on wars waged in the digital realm

In his 2016 book, *The Hacked World Order*, cyber security expert Adam Segal '90, PhD '00, detailed the impact of recent online attacks conducted by the United States, China, Russia, and other nations—from America's malware assault on Iran's nuclear program to North Korea's leak of sensitive e-mails stolen from Sony Pictures. By the time a second edition came out a year later, he needed to add a lengthy afterword to address alleged Russian interference in the 2016 U.S. presidential election. And now, with state-sponsored cyber operations regularly making headlines, Segal says he could probably write another 100 pages. "When I first started doing this cyber work, there might have been a story once a month that people would be familiar with," he says. "Now it's every week."

As director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, a nonpartisan think tank based in Manhattan, Segal is in the vanguard of this ever-expanding field. In an interview with CAM in his book-lined office at the Council—headquartered in a landmark building on the Upper East Side—he explains that the organization takes no positions on policy, but employs specialists like him to research and analyze complex global matters. As Segal puts it, his job is to help government officials, business leaders, journalists, educators, and others better understand the latest battleground in geopolitics: cyber warfare.

Segal's job is to help government officials, business leaders, journalists, and others better understand the latest battleground in geopolitics.

To that end, he has testified before Congress and conducted briefings on Chinese cyber espionage with the Joint Chiefs of Staff, the State Department, the Office of the Director of National Intelligence, and the Department of Commerce. He has advised lawmakers on how to revise policies that allow foreign investment in U.S. businesses while better protecting America's cyber security. He frequently offers his expertise in the media—including CNN, NPR, Fox News, the *Washington Post,* the *Wall Street Journal,* and the *Financial Times*—addressing topics from WikiLeaks to Silicon Valley's ongoing conflict with law enforcement over data privacy. Segal writes for *Foreign Affairs*, CFR's influential magazine, and contributes to its *Net Politics* blog. He also leads the team that created the Cyber Operations Tracker, a database of publicly known state-sponsored incidents that have occurred since 2005. According to the tracker, more than sixty such attacks struck around the globe in 2018 alone. "Everything ❯

PHOTO: SHUTTERSTOCK/PABLO LAGARTO

ADAM SEGAL
THE
HACKED
WORLD
ORDER
HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE

North Korea hit with sanctions for Sony hack

Pentagon, NSA seek to alter cyberwarfare strategy

Online attacks on banks raise fear of state backing

200,000 voters likely hit in elections cyberattack

THINK TANK (from left): Segal outside the Council on Foreign Relations on Manhattan's Upper East Side; his most recent book; cyber warfare in the headlines

is moving incredibly quickly," says Segal, who also serves as the Council's Ira A. Lipman Chair in Emerging Technologies and National Security. "It's hard to keep up with what's happening now, much less think about what's coming next."

Take Russia's hack of the Democratic National Committee and that nation's disinformation campaign during the 2016 election, which caught even Segal by surprise. He knew Russia was capable of such acts, since it had waged similar operations against Ukraine not long before. Yet Segal says targeting America in this way took cyber war to another level. "We had now entered a world where clearly all states were going to do this to each other as much as they could from now on," he says. "This was the new normal." And Segal warns that China poses an equally troublesome threat. He points out that entities associated with the Chinese government have broken into computer networks at the Pentagon and other U.S. agencies, stolen trade secrets from American companies like Coca-Cola and Google, and more. And while China hasn't yet tried to use cyberspace to sway American elections, he says it has launched online influence operations against activists in Hong Kong, Tibet, and Taiwan. As Segal wrote in an op-ed for the *New York Times* last fall: "China has both the playbook and the capacity to interfere."

Unsurprisingly, Segal says that there are no easy solutions to combat these cyber attacks. While the U.S. has brought criminal charges against suspected Russian and Chinese hackers and has imposed economic sanctions on those countries and others for online attacks, he doubts these moves will deter future assaults. He argues that America needs to shore up its cyber defenses in both the public and private sectors, recommending that counterintelligence officials identify vulnerable companies and help strengthen their computer security. If an influence campaign should occur, Segal says, the government must move swiftly to counter the spread of false information. He also thinks the U.S. should be partnering with allies—as well as engaging with adversaries like China and Russia—to agree upon international rules of behavior in cyberspace. "Unfortunately," he says, "not much of that is going on right now."

A government major on the Hill, Segal taught English in Taiwan and China for a year after graduation. He earned a master's degree in international relations from Tufts before returning to Cornell in 1993 to pursue a doctorate in government. His dissertation, which focused on high-tech enterprises in China, turned into his first book, *Digital Dragon*. For that project, Segal interviewed dozens of tech entrepreneurs, including managers at the then-nascent Huawei Technologies, now the world's biggest provider of telecom equipment and a hot topic in today's news. (The Trump Administration is currently attempting to block use of Huawei's products, claiming they present a cyber security risk that China can exploit for espionage or sabotage.) Segal's PhD advisor, Peter Katzenstein, the Walter S. Carpenter Jr. Professor of International Studies, says his former student was prescient about China's potential to become a tech superpower.

'Everything is moving incredibly quickly,' says Segal. 'It's hard to keep up with what's happening now, much less think about what's coming next.'

"His thesis was daring in some ways, and he succeeded in making it an interesting, cutting-edge book," says Katzenstein. "It really laid the foundation for his career."

Segal next served as an arms control analyst for the Union of Concerned Scientists—writing about missile defense, nuclear weapons, and Asian security issues—before joining CFR in 2001. Going forward, he foresees the need to address more sophisticated technologies like "deep fakes," the more realistic and harder-to-debunk video and audio content enabled by recent advances in machine learning, which Segal says is a looming menace. "It's another tool in influence operations—and right now, there's no technological solution," he says. "It's very worrisome." ■

— Heather Salerno

PHOTO: JOHN ABBOTT