SECURE TOMORROW SERIES

SCENARIO NARRATIVE 4: A NEW WAVE OF COOPERATION

The Cybersecurity and Infrastructure Security Agency (CISA) has produced these scenarios to initiate and facilitate discussion. The situations described here are hypothetical and speculative and should not be considered the position of the U.S. government. All names, characters, organizations, and incidents portrayed in these scenarios are fictitious.

YEARS IN THE MAKING PODCAST TRANSCRIPT

TITLE: "CCC and D-USA: A new wave of cooperation among unlikely allies"

Hosted by Philippa Roth; produced by Naveen Mehta, Sandra Chung, and Greg Jackson

Monday, October 25, 2026

Philippa Roth (PR): Hello and welcome to the "Years in the Making" podcast from the *Phoenix Post,* where we discuss how past world events built to significant turning points in history in retrospect. I am your host Philippa Roth, and today we will be talking about the new wave of cooperation occurring in cyberspace—including data security, interoperability, standardization, and digital identity—that we've witnessed over the past three years between countries, members of Congress, and private sector companies.

We're joined by Jacques Viltard, the former U.S. Ambassador to the European Union, and Dr. Naomi Marmer, a national security analyst focusing on technology and cyberwarfare at the Center for Analysis of Security and Peace in Washington, D.C. Both played key roles in negotiating the Cooperation in the Cyberspace Convention (CCC). Ambassador Viltard also testified before Congress on a hearing focused on digital privacy prior to the passage of the Digital U.S. Act (D-USA).

Ambassador Viltard, Dr. Marmer, thank you for joining us today.

Jacques Viltard (JV): Thank you for having me.

Naomi Marmer (NM): It's great to be here.

PR: So, let's get right to it: How did we get here? If we turn back the clock to the beginning of this decade, I think some of the things our listeners may remember most are the SARS-19 pandemic, political polarization in the U.S., strained trade relations with China, and Black Lives Matter. Coming from what seemed to be such troubling and divisive times, how did we end up in a "golden" period of global cooperation that we arguably haven't seen since the twentieth century? Ambassador Viltard, perhaps we can start with you.

JV: Certainly. I think we have a classic case of "things will get worse before they get better" here. A few events come to mind, starting of course with the SARS-19 pandemic. I would like to acknowledge first that the SARS-19 pandemic, like Hurricane Katrina in 2005, like the September 11 attacks in 2001, forced us to be more introspective as a nation. The hundreds of thousands of deaths, the rapid spread of the virus in certain communities and industries, the long-term economic ramifications of public health orders, and the distribution of vaccines brought out the already-present socioeconomic disparities. What people sometimes forget now is that the SARS-19 pandemic also

represented a turning point for our reliance on the internet. You had a sudden surge in remote work and online learning, both of which presented new targets of opportunity for malicious actors. We saw large-scale cyberattacks on hospitals and schools that left thousands without access to critical care and compromised student data. Once the widespread SARS-19 vaccine rollout began in 2021, there was a series of ransomware attacks on vaccine distributors by Fancy Bear in the U.S., EU, Brazil, and Canada. While all of this was happening, the U.S. was figuring out how to respond to the Multiplicities hack.

PR: Yes, the Multiplicities hack was one of the most extensive breaches at the time, compromising many government agencies and private companies. Dr. Marmer, how did the U.S. react to the hack?

NM: You know, at the time, the U.S. reaction was fairly by the book. The President imposed additional sanctions against Russia and froze accounts of oligarchs close to Putin to put Russia under further financial strain. The State Department also expelled diplomats and pressured allies to do the same.

PR: So, nothing out of the ordinary.

NM: No, and all of this made sense—they viewed Multiplicities as a classic act of espionage, which the U.S. also engages in when it is in our self-interest. You'll recall the U.S. and Israel interfering in Iranian nuclear operations over the years. A few prominent U.S. policymakers were initially advocating for a more retaliatory approach to the Multiplicities hack, but nothing really came of it—at least, nothing publicly known. These are all calculated moves. The U.S. ran the risk of escalating things further and revealing our cyber arsenal. Public polling at the time showed that the country was against a retaliatory approach to Multiplicities because no one saw any tangible impacts of the hack on life or property. It wasn't until Russia interfered with Ukraine's natural gas supply in 2022 that Russia finally crossed the line.

PR: That's right. What led Russia to act this way? And how did the international community respond?

JV: At the time, Putin was under tremendous political strain. Russia was feeling the burden of sanctions and still trying to recover from the SARS-19 pandemic. So as a way to distract the Russian people and rally support, Russia inflamed tensions with several adversaries, such as interfering with Ukraine's natural gas supply. This left the EU scrambling to meet its energy needs for a number of days. Unfortunately, the attack didn't trigger a united NATO response because Russia acted through a cyber-espionage group with close ties to its military to leave room for plausible deniability. Putin maintained that some rogue actors were to blame, but as far as I am concerned it was very clear from forensic evidence that it was Russia. No hackers have sufficient incentive—let alone funds and resources—to engage in an attack of this scale and difficulty without state sponsorship.

NM: The Ukraine hack and the resulting energy disruptions were really a step too far for many world leaders. Once Europe as a whole visibly saw and felt the impact of the Ukraine cyberattack on its day-to-day operations, countries like Germany and France adopted Russia's middleman playbook and began to engage in a deliberate yet measured tit-for-tat response against Russia. For example, there was a cyberattack in the Ysyk-Ata district of Kyrgyzstan, where a Russian airbase is located, that left the district without power for 48 hours. This went largely unnoticed by news media, but definitely signaled to Putin that the West was no longer going to tolerate Russian intrusions.

I believe it created a broad appreciation that the world was in a "mutually assured disruption" environment, where if such tit-for-tat cyberattacks were to continue escalating, everyone was set up to lose. This brings us back to Ambassador Viltard's "things will get worse before they get better" point. This prompted the U.S., Russia, China, the EU, and UK to negotiate and sign the Cooperation in

Cyberspace Convention (CCC) in 2023, codifying norms against nation-state cyberattacks. The CCC is really an important convention because it set redlines, created a forum through which countries could address cyber disputes, and established a sort of collective accountability that didn't exist previously.

PR: That's really interesting. So, it was the environment of "mutually assured disruption" we found ourselves in that served as an opening for unlikely bedfellows to come together and sign a convention.

I want to move to a different area of cooperation: the 2023 International IT Experts Forum. Ambassador Viltard, could you walk us through why the forum even took place and why it's seen as so instrumental to improving technology and user experience?

JV: Definitely. Your listeners might have noticed emails from various service providers detailing improvements to data privacy and security standards, interoperability changes, and the like. All of this is a result of the forum. For decades, the private sector, especially multinational corporations, has struggled to maximize the use of its data because each country had established its own unique set of data privacy, cybersecurity, and data governance requirements. In the past five years alone, data localization efforts by the EU and India have been creating a lot of headaches when it comes to international data transfers and slowing down service.

I believe the ratification of CCC signaled to the private sector that this was an opportune time for change. So several of the major tech companies convened a forum with academics, ethicists, lawyers, and CIOs and after more than a month's worth of deliberation produced standards that increase interoperability and data sharing among companies, integrate differential privacy, improve security, and promote ethical use of data. These, of course, were voluntary standards and not as strong as any government directive. But to the surprise of many of us, enough companies did agree to start phasing in these standards so that by 2024 they reached a critical mass. User security and privacy have increased dramatically over the past few years and I expect to see additional benefits moving forward.

PR: Yes, experts have applauded the forum, saying it has acted in tandem with the Digital U.S. Act (D-USA) to protect user privacy, increase security, and provide other benefits. I'd particularly like to get your thoughts here, Dr. Marmer.

NM: I think that's a fair assessment. D-USA, which is essentially our national data security and privacy protection law, adds the government-directive element, at least for American firms, which Ambassador Viltard was referring to. Passage of D-USA has been significant for several reasons: one, it is a testament to the new cooperative efforts we've seen across the political aisle and among countries and industries over the past few years. If you told me in 2020 that we'd have an American version of the General Data Protection Regulation by 2023, I wouldn't have believed you because of the sheer gridlock and disagreement over key issues, such as user control over personal data, regulation of third-party data brokers, and so on. The International IT Experts Forum ended up resolving some of these disagreements for Congress with a collective, industry-wide move toward standardization. Take differential privacy, for instance. This would have been a highly contested issue, but congressional members didn't need to negotiate much to protect the interests of organizations operating in their jurisdictions because these companies were already in agreement with one another on the path forward.

Additionally, D-USA, took the recommendations of the 2020 Cyberspace Solarium Commission report to heart, and set out to overhaul the government's privacy and data security regime and allocate

resources to achieve these goals. This was a direct response to the Multiplicities hack, which was a colossal failure of U.S. cyber defense systems. Congress realized the extent to which U.S. government agencies and critical infrastructure companies were lagging behind in their data security, privacy, and governance efforts. So, it created a National Cybersecurity Assistance Fund to provide funding for research and created additional opportunities for public-private collaboration in these fields, one of which is the four-year employee exchange between tech companies and government agencies.

PR: Yeah, I think the public has taken to this effort quite well, especially the digital identity cards and how much they've helped improve customer service.

JV: I agree. And for your listeners who might not have received their digital identity card yet—they are a part of the privacy and security regime overhaul we've been discussing. Many Americans started to receive them a year ago. They have been pointed to as having helped reduce red tape, get easier access to government services, and resolve disputes with agencies more quickly. I suspect a full rollout will also address issues ranging from identity theft to helping provide a smoother Transportation Security Administration experience at the airport.

PR: Would you agree that this new cooperative environment, coupled with increased research funding, has accelerated improvements in 6G, Internet of Things (IoT), and Artificial Intelligence (AI)-enabled technologies?

JV: Yes, definitely. The advancement in those technologies also benefited from the 2020 antitrust lawsuits in the U.S. and Europe against FaceMe and Dongle. Since then, companies have largely stayed away from predatory practices, such as acquiring emerging competitors, to remain under the Justice Department's radar and avoid scrutiny. So, the tech industry benefitted from smaller companies being able to raise funds, recruit talent, and use a number of high-quality datasets, which were made available following the forum and D-USA. All of these factors really helped diversify the tech industry by lowering the barriers to entry and enabling more innovation in 6G, AI, and IoT.

The diversification of the tech industry and increase in public funding have stimulated what I call "public good" advancements. Take the company Ethical AI, for instance, which provides algorithms to news media groups for fact checking, allowing them to debunk fake news much more quickly.

NM: Think about what that's done for our understanding and acceptance of truth and facts in the U.S.!

PR: That's a great point. I think it was a recent survey from the Khumalo Research Center that reported increased public trust in government institutions for the first time since the 1980s. Do you think these largely positive trends we have been discussing will continue?

NM: As much as I would like to give a definitive "yes," there are many areas in which the U.S. government and its allies have work to do. Take Iran, for instance. I briefly touched on the U.S. and Israel interfering in Iran's nuclear operations. I can tell you Iran isn't very happy; it's still recovering from the economic downturn resulting from the pandemic, struggling to control additional SARS outbreaks within its borders, and frustrated over sanctions. So, I suspect it will be a thorn in the U.S.'s side over the coming years.

JV: That's right—Iran is becoming nervous about its declining power in the Middle East, especially as more countries begin to normalize relations with Israel. Iran is looking to flex its muscles and reassert its dominance in the region. We've already seen it copy China and carry out cyber-espionage operations to advance its tech sector by stealing intellectual property and destabilizing other

countries, especially Iraq and Saudi Arabia. But I remain optimistic that the international community will remember what happened in Ukraine and prevent things from escalating further.

PR: Well, thank you both so much for your time. It's been a really interesting conversation. We hope to have you again on the show.

JV: It's been a pleasure.

NM: Thank you.