Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

ISSUE BRIEF

Confronting Transatlantic Cybersecurity Challenges in the Internet of Things

FEBRUARY 2017 BEAU WOODS

Introduction

In 2016, a series of highly impactful and publicized disruptions provided a wake-up call to societies on both sides of the Atlantic making obvious their dependence on inherently unpredictable technology. Just before the year began, a targeted attack disrupted the Ukrainian energy grid, forcing its operators to fall back on decades-old manual processes, and a similar attack followed late in the year. The Hollywood Presbyterian Hospital in Los Angeles was forced to shut down for weeks as a critical patient-care system was unintentionally disrupted by ransomware—a common plague that impacted many other parts of societal infrastructure through the year, including San Francisco's Bay Area Rapid Transit (BART), US electricity providers, and hospitals in the United States and across Europe. At the same time, a botnet of poorly secured devices disrupted large portions of the US Internet and knocked more than one million German households offline. And while the Russian breach of the Democratic National Committee (DNC) and the associated influence campaign continue to shock many in the United States and beyond, the specter of hackable voting computers also cast doubt on the US electoral system in the lead-up to and aftermath of the presidential election.

These events illustrated a general trend of increasing risk, from an increasing number of adversary types. High-capability adversaries, such as Russia, showed growing willingness to engage in cyberattacks. Meanwhile, high-intent adversaries, such as cyber-criminal groups and the Islamic State of Iraq and al-Sham (ISIS), have access to increasingly sophisticated toolkits to strengthen their capabilities. The line between nation-state and non-state hostility in cyberspace is blurring, while the United States and its allies are becoming more susceptible to adversaries of all types. Society is only one cyber crisis away from proving how unimaginative policy makers have been.[1] In the face of high-consequence cybersecurity failures, a higher standard of care is merited.

Against this backdrop, the Atlantic Council's Cyber Statecraft Initiative of the Brent Scowcroft Center on International Security, in collaboration with the Howard Baker Forum and CSC, initiated a series of conversations

The focus of the **Cyber Statecraft Initiative** is to examine the overlap of national security, international relations, and public safety to provide practical and relevant solutions to challenges in cyberspace. The Initiative works with Fortune 500 companies, governments, and other stakeholders to promote thought leadership in cyber statecraft—the key tool to generate innovative solutions for a free and resilient digital commons. The Initiative covers topics at the intersection of technology and the human condition, such as the impact of cybersecurity on public safety and economic stability and the growing importance of postnationalism with the emergence of new, powerful actors in this sphere.

1 Fran Burwell, Distinguished Fellow at the Atlantic Council, made this observation. Used with permission.

on these uncomfortable topics, anchored by dinners in Berlin in November 2016 and in Brussels in January 2017. These off-the-record discussions with policy makers, private sector leaders, academics, and cybersecurity researchers were meant to identify ways to confront cybersecurity challenges facing the transatlantic community, in 2017 and beyond. This issue brief synthesizes key observations, insights, and approaches from the series. The emergent theme was that the transatlantic community must come together at this critical moment in history to preserve trust through trustworthiness with cyber hygiene, societal and technical resilience, market transparency, and people-to-people connection.

> "... [T]he transatlantic community must come together at this critical moment in history to preserve trust through trustworthiness"

Public Safety and the Internet of Things

Connected technology holds both great promise and great peril for international security, prosperity, and stability. Increased integration of technological and social systems unlocks new capabilities for prosperity, growth, health, safety, and resilience. The Internet of Things (IoT) is bringing life-changing capabilities to more people, faster and cheaper, than would be possible otherwise. Public safety and human lives are improved by automotive safety features, medical therapies, logistics enhancements, utility services, and other advances.

At the same time, societies' dependence on connected technology is increasing faster than their ability to build defensive capabilities and resilience against accidents and adversaries. This dependency represents potential threats to: national and international security, where low-capability adversaries like terrorists and hacktivists gain new capabilities to cause physical harm; trustworthiness of democratic institutions, where poor cyber hygiene contributes to undermining confidence in the electoral process; and stability of global prosperity, where cybersecurity incidents reveal unreliable technological dependencies in key market segments.

Where cybersecurity failures impact human life and public safety, the consequences will manifest much more broadly. Exotic sources of potential harm, such as aviation disasters or terrorism, play an outsized role in shaping consumer confidence in key markets. Similarly, national security depends on reliable transportation, energy, and military capabilities—all of which are rapidly adopting technology and the associated vulnerabilities. Where cybersecurity impacts public safety—cyber safety, as framed by the Atlantic Council's Cyber Statecraft Initiative—the level of care must be commensurate with the level of harm.

Global supply chains and markets make IoT issues inherently international. Concern for public safety, prosperity, and national security transcends borders and unites international citizens and governments. Laws in one jurisdiction impact suppliers and consumers in distant reaches of the globe. Trust built by states, cooperating where their interests and incentives are aligned, can facilitate more trustworthy dialogues on other issues that might otherwise be contentious.

A Technical Literacy Gap

There exists a policy knowledge gap in connected technology and the Internet of Things. Information technology and the Internet are relatively new fields, and doctrine is still being formed. The growing dependence on the Internet of Things further widens this gap, as even cybersecurity and cyber-policy experts have struggled to come to grips with this new wave of connected technology.

Policy makers and other stakeholders vary widely in their cybersecurity background and their access to consistent, credible advice. Predominant mental models for understanding these technologies are inconsistent, and even the most faithful analogies diverge from technical fact in key areas. Policy makers' current ability to collectively anticipate, identify, and address cybersecurity issues, is therefore inadequate. There are four key aspects to consider in evaluating the impact of the IoT wave on cybersecurity: a cognitive cultural gap that has emerged due to three waves of connectivity; increased scale of the attack surface; added complexity for defenders, due to the diversity in functionality and security approaches; and increased potential to transfer the impact of cyberattacks from the virtual into the physical domain (i.e., increased

The Atlantic Council's Cyber Statecraft Initiative, in collaboration with the Howard Baker Forum and CSC, convened dinner discussions on increasing risks in cybersecurity in Berlin, Germany in November 2016 and Brussels, Belgium in January 2017. *Photo credit*: Runner1928/Wikimedia (Left), Diana Popescu/Wikimedia (Right).

potential for physical damage).[2] Based on these principles, it would be instructive to expand on this framework and extend it more broadly to identify material differences between cyber safety and more conventional domains.

- **Cultural Cognitive Gap**—Connected technology has undergone no fewer than three distinct generational shifts over the past thirty years. Cognitive capacity to understand and adapt to those changes cannot keep pace with the need for technically literate policymaking. Cultural practices and awareness may take even longer to identify and adjust to optimal mental models.

- **Scale of Attack Surface**—The number of distinct hardware and software components in connected technology often exceeds the ability of one person to identify, account for, and understand implications. Connectivity brings many orders of magnitude more interactions, with more potential hazards or hostile actors. In combination, the number of vulnerable, exposed components exceeds societies' ability to anticipate, particularly in a domain that changes so quickly.

- **Complexity**—Connected technologies have vastly different composition, economics, operational environments, and timescales. Limited capabilities and economic considerations in IoT constrain options for securing these systems, while operational contexts may require more rigorous and preventive approaches than have yet been achieved even in traditional information technology. Timescales can be more extreme in IoT as well, with lifetimes measured in decades rather than years, and irreparable harm can manifest in milliseconds.

2 This framework was volunteered by Ambassador Sorin Ducaru, Assistant Secretary General of NATO for Emerging Security Challenges. Used with permission.

- **Consequences**—When safety-critical systems rely on software and connectivity, cybersecurity failure modes include direct harm to human life and public safety. Public unfamiliarity with the causes, bounds, and extant efforts can amplify impact on trust in markets and governments. Widespread dependence on these technologies in critical infrastructure poses a national security threat, if those technologies remain vulnerable and exposed to adversaries who can use these systems' scale, speed, and connectivity to undermine them.
- **Adversaries**—The Internet can bring adversaries from across the globe into private homes and critical public infrastructure, whereas only the world's superpowers could match that reach thirty years ago. Different adversaries have different goals, motivations, methods, and capabilities. While some adversaries may be chastened by potential harm from safety-impacting systems, others may seek those systems out. Low cybersecurity hygiene and high connectivity open the door for actors who lack others' skill and restraint (i.e., those who "like the boom").

Solutions to Transatlantic Cybersecurity Challenges in the Internet of Things

In the face of uncomfortable situations, it may be time to consider uncomfortable approaches. Among these, several seem most promising in bringing a level of care to match the level of potential harm. These approaches center on cyber hygiene, resilience, market changes, and people-to-people connection.

Hygiene-focused approaches to cybersecurity deny low-capability adversaries by raising the level of defense higher than they can overcome. Many of the highest-intent adversaries also have the lowest capabilities, yet they are still highly successful. Hacktivists generally do not have a high degree of skill, yet even their simple tactics achieve high profile consequences; ISIS has adapted and extended this playbook. State actors often use the tools and tradecraft of a much lower-skilled adversary to avoid tipping their hand and to confound investigators attempting to identify them. The technical tradecraft used in the Russian attack on the DNC was not much more sophisticated than Nigerian scam emails. Raising the bar causes higher-capability adversaries to increase resources and reduces the field of actors, increasing confidence in attribution. Many of these hygiene practices are captured in existing standards or are knowable by owners and operators.

Resilience can prevent harm and permit society to recover in the wake of a large-scale event. While some techniques focus on avoiding failure from cyberattacks, others ensure that any failures are evident and can be accounted for in operations. Awareness and education on smartly consuming information in the Internet era serves as an inoculation against information operations, and other measures can reduce the impact and time to recover at a societal level.

> "Dependence on connected technology is growing faster than societies' ability to secure it against the rising capabilities and intent of diverse adversaries."

Market transparency and software liability allow buyers to size and bound their risk, and can shape market choices. Owners and operators who can identify known points of risk, such as published software defects or configuration weaknesses, can account for these in planning and resourcing, to better defend themselves from cyberattack. Manufacturer attestation of security capabilities improves confidence in the brand and in entire markets. Liability regimes for public safety and software conflict in the Internet of Things; reconciliation of those differences guides manufacturers, business customers, and consumers to clearly define roles, responsibilities, and accountabilities.

Connecting people from different backgrounds and experiences in the transatlantic community shrinks the cultural cognitive gap. Many perspectives are compatible where knowledge, principles, and doctrine are nascent; policy makers and others are well served to optimize solutions for the multiple truths that make up reality in the Internet of Things. Accounting for the broad diversity of background, perspective, and experience builds better mental models, which allows the transatlantic community to generate and promulgate more effective policies.

Conclusion

Dependence on connected technology is growing faster than societies' ability to secure it against the rising capabilities and intent of diverse adversaries. The Internet of Things has great power to transform societies, but only if the trust placed in these technologies is merited. A public crisis of confidence may delay benefits for years or decades, and susceptibility to remote attack may undermine national and international security. Solutions call for engagement across the transatlantic community—to build bridges between disparate communities, to embrace preventive resilience, to realign market forces, and to return to effective cybersecurity practices. Where domains of expertise and areas of interest overlap, societies can preserve trust through trustworthiness and be safer, sooner, together.

Beau Woods is deputy director of the Cyber Statecraft Initiative at the Brent Scowcroft on International Security, where he focuses on the intersection of cyber security and the human condition, primarily around cyber safety. He also works closely with the I Am The Cavalry civil society initiative, ensuring the connected technology that can impact life and safety is worthy of our trust.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org