“Expertise at the Boundaries: Understanding Critical Infrastructure Cybersecurity”
by Rebecca Slayton, Cornell University, and Clare Stevens, University of Portsmouth

Critical infrastructure organizations around the world are increasingly connecting the operational technology (OT) that controls physical devices, processes, and events with the information technologies (IT) that comprise cyberspace. Many organizations seek the integration of OT and IT in order “to gain competitive advantage, become more efficient, profitable and reliable.”[144] However, this revolution also comes with new challenges and risks. Increased connectivity increases the complexity of large technical systems and the corresponding potential for “normal accidents.”[145] It also increases the risk of cyber-attacks. For example, in both 2015 and 2016, Russian hackers successfully shut down sections of Ukraine’s electric power grid. Though these attacks have been overshadowed by the physical attacks associated with Russia’s invasion of Ukraine, nations around the world are devoting growing attention and resources to the challenges of security that come with what the World Economic Forum has described as the “Fourth Industrial Revolution.”[146]

Historically, critical infrastructure organizations have secured operational technology primarily through physical isolation. Through most of the twentieth century, the computers controlling operational technology ran behind locked doors and tall fences, and thus needed few if any additional security controls. In fact, the lack of computer passwords or other computer security controls could be understood as a safety feature in the context of operational technology, because it ensured that operators would not be locked out in an emergency.[147] But as organizations have begun to connect these computers to broader networks that enable remote access, cybersecurity has become increasingly important. Unfortunately, implementing cybersecurity in legacy systems incurs production downtime and capital improvement costs that are expensive—sometimes prohibitively so.

Decisions about how to manage the integration of IT and OT thus entail trade-offs between different kinds of public goods and risks, including security, safety, reliability, and economy. These trade-offs are not merely arcane technical issues, but policy challenges that cross boundaries between governments, sectors, and fields of expertise. In this essay, we first outline the challenges of managing risks that span these traditional boundaries. We then focus on a challenge that underlies risk management across all of these boundaries: the challenge of creating credible expertise in a still-emerging area of technology that creates new opportunities for emerging threats. While policy often seeks to manage boundary-spanning risks from the top-down—with governmental policies shaping cooperation between public and private organizations, which in turn coordinate and structure the work of different kinds of experts—we argue for a bottom-up approach that examines how the cultural practices of experts alternately produce, maintain, navigate, and transcend boundaries.

Three Kinds of Boundaries: Governmental, Organizational, and Professional

The physical infrastructures associated with operational technologies often cross boundaries between and within different nations, creating interdependencies and complicating questions of responsibility. For example, the North American electrical grid is a giant system of systems spanning Canada, the United States, and Mexico. Similarly, in Europe the bulk transmission of electric power requires the cooperation of operators spanning from Eastern Russia to the Republic of Ireland, and this does not include the many thousands of distribution operators across the continent. Many critical infrastructures are also indirectly connected to more distant nations that produce critical components and flows of oil, gas, coal, and other materials. As a case in point, the European Natural Gas Network constitutes more than 200,000 km of transmission pipelines, over 2 million kilometers of distribution network stretching across the continent, and is operated by a complex combination of large private corporations and European government agencies.[148]

Regional and international organizations have created regulations that establish minimum levels of security. For example, in 2016 the European Union issued a Directive on the Security of Networks and Information Systems (NIS) that required member states to appoint national authorities to serve as a single point of contact for coordinating cross-border issues and to develop policy frameworks to ensure that critical infrastructure operators are implementing security safeguards that are proportional to risk.[149] Similarly, the United States has delegated authority to establish cybersecurity standards to an industry group, the North American Electric Reliability Corporation, which operates across the United States, Canada, and a small portion of Mexico.

These policies leave considerable ambiguity surrounding what constitutes an adequate response to cyber risk. Furthermore, many organizations fall out of the scope of regulation due to jurisdictional issues. For example, the United States regulates electricity production and transmission through the Federal Energy Regulatory Commission (FERC), which has the authority to establish both reliability and security standards. In the United States, however, electricity distribution is regulated by state and local agencies that have traditionally focused primarily on the economic and reliability needs of ratepayers, not national security.[150] Responsibility for cybersecurity and many other aspects of critical infrastructure thus remains diffuse, with unclear lines of authority.

A second set of boundaries lies in the split between the private organizations that often provide critical infrastructure, and the governmental organizations that are responsible for national security. This divide is particularly problematic in nations with strong traditions of privatization. For example, the majority of electrical power in the United States is produced by investor-owned utilities whose primary goal is to turn a profit for shareholders, not provide national security.

Nations in North America and Western Europe have attempted to align public goods such as cybersecurity with corporate interests through public-private partnerships, a term used to describe a broad range of organizational arrangements. Scholars warn that public-private partnerships are "no silver bullet," with continuing tensions and disagreement about appropriate arrangements for sharing information and delegating authority and responsibility for security.[151] Governments that are committed to free market principles have tried to make private organizations responsible for the security of their own networks, but this strategy becomes problematic when the threats to those networks are other state actors with a potential impact on national security. Indeed, most private organizations want to pass responsibility for protection from nation-state threats to the federal government.[152]

Because different kinds of threats use similar tactics, it is impossible to simply split responsibility for cybersecurity along these lines—delegating responsibility for defense against nation-states to the government, and responsibility for defense against criminals and less resourced threats to private organizations. Indeed, the lines between these different kinds of threats are themselves quite blurry; as Max Smeets notes in his essay for this forum, states sometimes act through or tacitly allow hacking by criminal organizations. Practical decisions about what security measures to implement, and at what cost, must be oriented towards defending against multiple kinds of threats, not just a few. Thus many governments have attempted to establish regulations to ensure that critical infrastructure organizations are managing security in a manner that is commensurate with risks not only to organizational goals, but also to national security. The diversity and complexity of critical infrastructure defies any one-size-fits all security solution. Furthermore, regulators lack the expertise and local knowledge needed to establish regulations that are can ensure security in the complex and variable contexts of critical infrastructure. As a result, regulations leave considerable discretion to private actors who must weigh tradeoffs between cost, reliability, and security.

This leads to the third boundary-spanning challenge: how can credible expertise be created in the newly emerging field of OT cybersecurity? Many industry observers note a gap between expertise in OT and IT—that is, between the practices of those who work with physical control systems and those who work with office-environment computers. The UK's National Cyber Security Centre (NCSC) explains: "Where cyber security for IT has traditionally been concerned with information confidentiality, integrity and availability, OT priorities are often safety, reliability and availability, as there are clearly physical dangers associated with OT failure or malfunction."[153] These different priorities require different rhythms and practices. Physical infrastructure changes gradually in order to maintain high levels of reliability and safety, but information infrastructure changes more rapidly.[154] Industrial control systems are expected to last for 25-125 years, while most information technology products are expected to last 3-5 years.

The fast-moving pace of information technology is both a vulnerability and a strength. Economies of scope accrue to information technology companies that capture an early market share, giving them a strong incentive to "ship it Tuesday, get it right by version three," i.e. to ship insecure products.[155] Without large incentives to develop more secure products, information technology companies rely instead on rapidly patching vulnerabilities as they are discovered. Patching can produce unexpected interactions with high consequences in industrial control systems, such as a loss of control over hazardous equipment. Organizations have traditionally scheduled industrial control systems maintenance months or even years in advance to ensure safe and reliable operation, but the need for frequent updating poses challenges to these practices.[156]

Unbounding Cybersecurity Expertise

In summary, IT communities have traditionally focused on security, while OT communities have focused more on safety, but policymakers are pushing for the integration of safety and security.[157] Over the past twenty-five years, engineers and regulators have tried to develop shared practices and standards to overcome these differences, but significant tensions remain.[158] The field of OT cybersecurity is still emerging at the point of new socio-technical developments. As Raj Badiani, the "Head of Digital" at Raytheon UK notes, "the OT cyber security maturity remains comparatively under-developed."[159]

Many discussions of the gap between OT and IT suggest a top-down approach to bridging these different areas of expert practice.[160] On the UK's National Cyber Security Centre blog, one "senior security architect" argues:

> ...operators should ensure that both OT and IT systems are equally and consistently accounted for in their overall approach to risk management. Not to do so could result in differences and deficiencies in the way cyber security policies are applied and risks are managed across an operator's combined IT and OT estate. […] The most effective operators are those where any friction between OT and IT teams has been reduced and where the overall approach to risk management is applied consistently in both IT and OT environments. [161]

The need to manage cultural differences, or "friction," between IT and OT communities is increasingly a feature of official and regulatory discourse. Industry observers note that "IT and OT exhibit widely-differing cultural values across several dimensions," suggesting that collaboration and coordination problems are inevitable.[162] Regulators often describe culture as a tool for achieving policy objectives. For example, the UK's Centre for the Protection of National Infrastructure argues that "getting security culture right will help develop a security conscious workforce, and promote the desired security behaviours you want from staff."[163]

Anthropologists and sociologists argue that culture is emergent, and thus cannot be used as an instrument to achieve engineering goals. Too often, talk of security or safety culture ignores competing interests and power differences within organizations.[164] This discourse frames humans as the weakest link, and obfuscates more fundamental structural problems and responsibilities for creating the problems that individuals must resolve.[165] Policies that focus only on essentialized differences or cultural stereotypes will likely produce efforts at top-down *coordination* that do not necessarily lead to effective on-the-ground *collaboration*.[166]

We argue for the need to study the situated practices that alternately produce, cross, and transcend these boundaries.[167] Sociologists of science have conceptualized boundaries between fields of expertise not as natural barriers to be managed, overcome, or erased, but as social constructs to be studied. For example, scientists often engage in "boundary-work:" rhetorical efforts to distinguish their work from that of non-scientists.[168] A key finding of this work is that socially-constructed boundaries shift with time and place. Others have examined how different fields of work coordinate their work through boundary objects: artifacts that take on distinctive meanings in different fields of activity, yet retain sufficient stability to enable coordination.

These studies suggest new research questions and strategies that go beyond efforts to engineer cultural cooperation from the top-down. How do experts rhetorically construct or challenge boundaries around their field of work, excluding or including insiders? What technologies and concepts have proven useful in coordinating fields of work that have traditionally been disparate? What interests are at stake in efforts to maintain boundaries between distinctive fields, and what interests are driving efforts to merge or overcome such boundaries? How do these interests and practices vary across national contexts, and how can an understanding of these distinctive interests inform regulatory guidelines and practices? Rather than attempting to engineer culture from the top-down, we need to better understand how experts construct and navigate boundaries around their areas of expertise.

Conclusion

Critical infrastructure cybersecurity is a "wicked problem" of coordination among multiple nations, sectors, organizations, occupations with highly complex interrelationships.[169] As other scholars have argued, "[a]ny understanding of resilience, the dynamics that produce safety, on a societal level needs to be based on study of work practices that cross organizational boundaries."[170] We argue for research that examines how the expertise is constructed as workers negotiate these boundaries. How do these experts generate credibility and authority in the workplace, and to decision makers in the private sector, and to policymakers? In contrast to managerial or structural approaches that attempt to coordinate culture from the top down with formalized frameworks and protocols, a focus on how workers generate authority through and across different boundaries can help us better understand the processes that go into managing resilience.

"Expertise, Authority, and Rulemaking in the Internet's Infrastructure"
by Jesse Sowell, University College London

Introduction

As the conflict between Russia and Ukraine escalated in March 2022, Ukraine asked technical communities that coordinate critical Internet resources to effectively disconnect Russia from the Internet, ostensibly to limit Russian propaganda and disinformation campaigns.[171] Both the Internet Corporation for Assigned Names and Numbers (ICANN, the organization maintaining top-level domain name services) and the Regional Internet Registries (RIRs, organizations delegating IP addresses necessary for Internet communication) declined to intervene.[172] Perhaps anticipating the request, the Executive Board of the Réseaux Internet Protocol Européens Network Coordination Centre (the RIPE NCC: the RIR that serves Europe, the Middle East, and Russia) had just issued a resolution reaffirming longstanding norms that the "means to communicate should not be affected by domestic political disputes, international conflicts or war."[173] The *Resolution* further highlights that "the RIPE NCC can be trusted as authoritative and free from bias or political influence" precisely because it "guarantees equal treatment for all those responsible for providing Internet services...across a diverse geographical and political region."[174]

Although triggered by the "high politics" of international conflict, the norms and assertions of authority at play in the *Resolution* have been historically relegated to the "low politics" of technical coordination.[175] Despite RIRs central role in Internet governance and security, scholars have devoted far more attention to more prominently visible organizations such as ICANN and the Internet Governance Forum (IGF), with the result that many scholars and government officials treat these organizations as the familiar, de facto Internet governance bodies.[176] Michel J.G. Van Eeten and Milton Mueller critique this focus as "lamppost science," challenging scholars to find Internet governance among the "heterogeneous organizational forms" and "massively distributed authority and decision-making power" that contribute to managing a complex, decentralized, and distinctly global Internet.[177]