Special Issue Article

Science, Technology, & Human Values
2024, Vol. 49(4) 827-850

DOI: 10.1177/01622439241240411
journals.sagepub.com/home/sth


Unscripted Practices for Uncertain Events: Organizational Problems in Cybersecurity Incident Management

Ashwin Jacob Mathew[1]

Abstract

Scripts can help us understand the designer–user relationship, by offering analysis of designers' intent in technological objects and examination of users' behaviors through willingness (and unwillingness) to take on scripts. But how are we to understand these relationships in the context of cybersecurity, in the face of adversaries determined to gain unauthorized access to computer systems by actively subverting scripts? In effect, cybersecurity attacks involve re-scripting of computing systems to gain unauthorized access through unscripted features of these systems. Cybersecurity attacks are always uncertain events: attackers can never be certain when re-scripting will be successful, and defenders can never be certain when or where to expect an attack, as unscripted features are difficult to know until they are exploited. In this paper, I study practices of cybersecurity

[1]Department of Digital Humanities, King's College London, United Kingdom

Corresponding Author:
Ashwin Jacob Mathew, Department of Digital Humanities, King's College London, London WC2R 2LS, United Kingdom.
Email: ashwin.mathew@kcl.ac.uk

incident response to examine how cybersecurity engineers respond to the novel attacks they encounter daily. I show how these are fundamentally *unscripted practices* emerging in response to *unstable scripts*, structured through the uncertainties inherent in cybersecurity engineering practice. The improvised practices and changing networks of social relations which I trace demonstrate the limits of stable scripts and provide new tools for analyzing unstable scripts.

Keywords
scripts, internet, cybersecurity, uncertainty

Introduction

Ever since Akrich's (1992) influential formulation, scripts have provided a powerful analytic for understanding how technological objects mediate the relationship between designer and user. Designers imagine abstract users, *inscribing* idealized scripts for the use of technologies into the design of objects. When users encounter technological objects, scripts are negotiated in a process of *de-inscribing*, since idealized scripts rarely align with the reality of use. To ensure their function, technological objects must "stabilize and channel" (Akrich 1992, 220) the tension between inscribing and describing, creating a functioning system by resolving disagreements between designers' intent, and the practices of users and other actors.

But what if the function of a technological object, and the script itself, is defined in fundamentally opposed terms by different groups of actors? This is the situation we find in cybersecurity. Attackers seek to destabilize computing systems, even as information security teams work to ensure the stability of these systems in the face of ongoing attacks. Under these conditions, there is no negotiation that can lead to a stable system, as the idea of stability itself becomes open to definition. For defenders, following the classic information security formulation, a "stable" system is one that maintains its confidentiality, integrity, and availability (Samonas and Coss 2014). For attackers, a "stable" system is one for which they have compromised or disrupted these properties, whether by exfiltrating sensitive data (violating confidentiality), by manipulating the function of essential systems (violating integrity), or by denying access to systems (violating availability).

The inability to negotiate stability in the practice of cybersecurity is made worse by the fact that new kinds of attacks are constantly emerging,

some of which (so-called zero-day attacks) may remain unknown to defenders and open to exploitation for extended periods of time (Bilge and Dumitraş 2012). The result is an indefinite arms race between defenders seeking to protect their systems against known attacks, even while monitoring for and responding to new kinds of attacks, and attackers constantly probing systems to find new ways to disrupt and compromise their security. The complex interdependent nature of modern computing systems generates additional concerns, as these systems compose infrastructures typically assembled from a variety of components and services provided by different vendors, each with their own distinct risks and potentials for vulnerability to attack. In consequence, successful attacks are near-inevitable but always uncertain events (Bambauer 2014). This situation is compounded by the possibilities for the deception that are intrinsic to cybersecurity (Gartzke and Lindsay 2015, 2017), as attackers may hide their presence by subverting information systems (e.g., to maintain ongoing capabilities to exfiltrate sensitive data), rather than making their presence visible through overt action (as in the case of denial of service attacks). Operating in an environment that provides hardly any semblance of stability for sociotechnical systems and associated scripts, cybersecurity is founded upon what I term *unstable scripts*. In contrast to Akrich's argument that stability is necessary for the functioning of sociotechnical systems, the concept of unstable scripts calls to attention conditions in which systems function despite ongoing irresolvable instabilities.

It is entirely possible that different scripts with differing interpretations of stability might coexist within the same system, while not necessarily rendering a system unstable across various uses. However, instability in cybersecurity has a particular character that stems from fundamentally opposed interpretations of stability generated by attackers and defenders, and from the complex and mutable materiality of computing systems, creating potentials for radical contingency and constant change. In consequence, it is easy to imagine cybersecurity as an anarchic enterprise in which the only constant is instability. Yet for the most part, the online services that we use every day appear stable, whether our personal use of social media, search engines, and so on or our professional use of organizational computing systems. The seeming contradiction between the stable everyday experience of online services, and the adversarial environment of cybersecurity raises an important question: How is the appearance of stability in the scripts of online services constructed over the unstable scripts of cybersecurity?

I explored this question through a yearlong ethnography of the practices of information security teams in five university campuses in the United

States. As I discovered, the work of cybersecurity is at once exciting and mundane. Information security teams must fit into predictable, stable organizational structures and processes, while at the same time being oriented toward dealing with uncertain, destabilizing threats. Nowhere is this truer than in cybersecurity incident management—the practices involved in anticipating and responding to attacks—which I focus on.

Scripts have previously been used to examine relationships in cybersecurity, by integrating attackers into actor networks (Pieters 2011), in evaluating organizational security policies governing employees (Pieters et al. 2013), in analyzing privacy (Coppens, Veeckman, and Claeys 2015), in evaluating user development of software (Karlsson and Hedström 2014), and in examining the events reconfiguring an actor network that led to a security breach (Hedström, Dhillon, and Karlsson 2010). Feenberg (2019) employs-related concepts of programs and anti-programs (Latour 1990) to theorize the power relations that construct the internet, including those related to cybersecurity. Although adversarial relationships are studied across these works, their focus is on using scripts/programs to think about cybersecurity, rather than examining the implications of cybersecurity for theorizing scripts/programs. By contrast, I argue that the unstable scripts of cybersecurity create conditions in which we must reconsider the scripts themselves.

Following Akrich, although scripts may be contested, they are expected to eventually arrive at a stable state to allow a sociotechnical system to function. In contrast, I argue that scripts in cybersecurity are inherently unstable, demonstrating conditions under which stable scripts find their limits in the analysis of sociotechnical systems. An unstable script seems a contradiction in terms—but by examining this contradiction and how it is sustained, we may arrive at new insights into the nature of scripts. Unstable scripts in cybersecurity do not imply anarchy. Rather, they require analyzing the *unscripted practices* through which instability, uncertainty, and adversarial relationships are integrated into sociotechnical order.

In the following section, I explore the relation between understandings of stable scripts and ideas of unstable scripts and unscripted practices central to my analysis. Next, I provide a brief note on methodology, before moving on to my ethnographic account, which proceeds in three parts. I begin by studying how cybersecurity concerns overflow scripts, then examine how uncertainty in cybersecurity is managed within organizations in the face of unstable scripts, and close by showing how knowledge for cybersecurity is built from improvised networks of sociotechnical relations constructed within and across organizational boundaries. Together, these form the basis

for my analysis of unscripted practices in cybersecurity, which I present in the concluding section.

Unstable Scripts

> It is only when the script set out by the designer is acted out—whether in conformity with the intentions of the designer or not—that an integrated network of technological objects and (human and nonhuman) actors is stabilized. (Akrich 1992, 222)

There has always been a possibility for resistance in scripts, albeit resistance that allows for eventual stability—even if a stability that strays from the designer's intent. Throughout Akrich's analysis, resistance to scripts is never marked out as irresolvable. While there may be disagreements between the designer's inscription, and the de-inscription acted out in uses of a technology, there must be a resolution of these disagreements for a system to function or at least differing interpretations of stability that are capable of mutual coexistence in a "multistable" system (Rosenberger 2014). It seems almost a truism: if a system is riven by irreconcilable disagreement, how could it function at all?

Yet irreconcilable disagreement is exactly what we find in cybersecurity. I employ three key concepts to analyze this irreconcilable disagreement in relation to scripts. First, networks of relations mediated by scripts are structured through *adversarial* interests, as attackers and defenders of computing systems constantly seek to counter each other. Second, there is *uncertainty* in how new scripts will be developed and subscribed to by different actors in the attempt by attackers to exploit previously unknown—or unnoticed—vulnerabilities, and efforts of defenders to anticipate and improvise responses to these attacks. Finally, systems are subject to *instability* when opposition between scripts remains fundamentally irresolvable, as is the case in cybersecurity. I examine each of these three concepts in relation to scripts to understand how cybersecurity engineers engage in their work through *unscripted practices*.

Instability

To develop my conception of unstable scripts, I begin by disaggregating what I consider to be three related varieties of instability in scripts—interpretive, creative, and adversarial—of which I am most concerned with the last.

Interpretive instability is that which we find in Akrich's original framing and related work, which is concerned with how actors negotiate differing interpretations of scripts. There is uncertainty as to how disagreements among actors will be resolved, and what the eventual stable form of the system that will be achieved may be—yet stability (however fleeting) must be achieved to enable a functioning system.

Creative instability applies when considering scripts in the context of art or innovation, which embeds uncertainty in the scripts themselves. As Akrich et al (2011, 195) put it, "Innovation by definition is created by instability, by unpredictability which no method, however refined, will manage to master entirely." Igelsböck (2016) develops the "innovation script" to theorize the tension between the unpredictable, unstable nature of innovation and organizational imperatives of predictability and stability that seek the apparently self-contradictory aim of well-managed, repeatable innovation processes. Innovation scripts embed within themselves possibilities for change through creative instability as they must "be expected to carry unscripted elements or even 'counter scripts' with them as a very part of the scripts" (Igelsböck 2016, 438)—although stability must still be achieved to deliver eventual products.

Adversarial instability arises from the irresolvable opposition of actors' interests, rather than from differing interpretations of scripts (interpretive instability), or from within the scripts themselves (creative instability). In my analysis, adversarial instability is distinctive in relying on security to enable the appearance of stability, even as security itself becomes both site and source of uncertainty. Von Schnitzler's (2013) study of the deployment of prepaid electricity and water meters in South Africa illustrates these issues well. Von Schnitzler employs scripts to understand the conflict between neoliberal regimes which frame water and electricity as market resources, and citizenship regimes which frame these as political rights, locating this conflict in the material form of the prepaid meter. Security is essential to Von Schnitzler's (2013) work, as citizens seek to bypass prepaid meters to ensure access to electricity and water, while infrastructure companies devise ever more secure meters to resist tampering. The result is an arms race through a series of "strategic scripts and counter-scripts—interventions in an ongoing series of low-intensity conflicts that have become materialized within the technology itself" (p. 687) which proceeds in "a seemingly endless cycle of innovation and subversion" (p. 688).

While there may be an overall (if uneven) stability in the water and electricity infrastructures that Von Schnitzler studies, this occurs against adversarial relationships between citizens and infrastructure companies,

uncertainty about the progressions of scripts and counter-scripts, and instability in the conflictual form of the prepaid meter. This mirrors the situation in cybersecurity, where adversarial relationships between attackers and defenders result in the constant generation of opposing scripts in conflict over control of computing systems.

To deal with uncertainty in cybersecurity, Slayton (2021) calls for attention to how actors are enrolled and cut out from actor networks—while also cautioning that not all ties can be cut, as this may impair the utility and security of computing systems. Whether in the material ties of network connectivity that provide necessary access to computing systems or in the ties with the variety of actors (such as cybersecurity companies) who can help secure computing systems, Slayton notes how cutting certain ties might, in fact, make a system less useful or less secure. Attackers exploit this tension, avoiding unenrollment by accessing systems through ties that can't reasonably be cut, and shifting their behaviors as networks are reconfigured in response to their activity.

As this discussion illustrates, unstable scripts are produced with the very mechanisms through which scripts are meant to be stabilized: networks of relationships (which incorporate irreconcilable adversaries) and material forms (which are the site of ongoing conflict).

Uncertainty

Unstable scripts in cybersecurity are not only caused by adversarial instability—they are equally a consequence of the materiality of computing systems which are the objects of attack and defense in cybersecurity. By their very nature, computing systems are designed to be customizable to fit the needs of users, acting as almost indefinitely repurposable tools that have been characterized as general-purpose technologies (Jovanovic and Rousseau 2005). Computing systems are intended to provide ongoing abilities to change their scripts through re-scripting to customize their scripts through programming and configuration. The uncertainty of attack and defense in cybersecurity is in no small part due to the possibilities for re-scripting that are intrinsic to computing systems, as both attackers and defenders engage in an arms race of ever more sophisticated scripts and counter-scripts to re-script the computing systems that form the material sites of their conflicts.

Re-scripting is generally understood to encapsulate actions taken to reimagine and modify an existing object with a new script. This approach has been employed in design workshops to re-imagine the function of consumer products such as digital cameras (Ward and Wilkie 2008; Wilkie

2020); to explore how artifacts are redesigned in use (Esfahani and Carrington 2015), for example, in a child's play with dolls; and to redesign artifacts with specific values in mind, such as femininity, truth, or reduction of food waste (Rasmussen and Petersen 2011; Mulligan and Griffin 2018; Plasil 2020). Behind these analyses lies the intention of actors functioning as designers to re-script artifacts that have pre-existing scripts that may resist such re-scripting efforts. Computing presents a significant contrast to these understandings because computing systems are designed to be flexible, with re-scripting as a primary design goal. Instability in cybersecurity is therefore a consequence of the mutability intrinsic to the materiality of computing, as much as a consequence of the adversarial relationships that generate incompatible understandings of stability.

The possibilities for re-scripting in computing are readily apparent in studies of creativity which examine scripts in the context of participatory "open world" games (Abend and Beil 2016) and in the development of software for artistic performance (Carey 2016). As Pollock (2005, 504) argues in a study of improvisation in the work of software programming, "to program is to perform work-arounds, to bypass constraints, and to rewrite code." Computing systems not only carry scripts to be negotiated between users and designers but also embed prospects for radical change, as their general-purpose material bases make the scripts of computing open-ended to re-scripting. Paradoxically, re-scripting provides the material capabilities through which computing systems themselves facilitate resistance against stable scripts, as attackers are able to employ re-scripting to subvert scripts in the function of systems, even as defenders re-script systems to mount responses to attacks. The potential for re-scripting in computing is benign—even productive—when viewed in the context of creative instability. However, when considering adversarial instability, re-scripting requires responses grounded in security to protect systems at risk.

In order to gain access to re-script computing systems, attackers exploit social and technological vulnerabilities that are unanticipated by defenders. I term these *unscripted features*: elements of a sociotechnical system that are not part of the system's script, but which are nonetheless integral to the system and which gain valence only when they are enacted as part of a new script within the system. Lannge and Borg (2021) present a similar idea, arguing that infrastructures are "multistable" (Rosenberger 2014), allowing a variety of scripted and unscripted uses to coexist in relation to the same material object. Michael (1996, cited in Pollock 2005) offers an oppositional perspective, arguing not only that technologies always embody multiple scripts that users may employ but that these multiple scripts are often

contradictory. Drawing from this insight, adversarial relationships will generate unstable scripts, as opposed actors devise scripts and counter-scripts from both scripted and unscripted features. Uncertainty is intrinsic to these disparate analyses, as unscripted features are unpredictable, untapped potentialities, remaining unknown until they are discovered and enacted—a point that Spencer (2021) makes well in conceptualizing cybersecurity vulnerabilities. Pelizza (2021) makes a complementary argument in describing "relevant knowledge" in information systems, which similarly remains an untapped potentiality until becoming salient when actualized in practice in particular situations.

My understanding of unstable scripts builds from a series of interrelated concepts: the potential for re-scripting intrinsic to the materiality of computing, unscripted features that provide fodder for the generation of new scripts, and adversarial relationships that produce opposing scripts and counter-scripts.

Unscripted features in cybersecurity range from easily exploitable vulnerabilities (such as sensitive user data inadvertently made accessible through unsecured web interfaces) to sophisticated attacks that require substantial investments of time and resources to discover and implement (such as zero-day vulnerabilities). Unscripted features are not planned by designers and therefore are not part of a system's script but remain latent potentialities that attackers may exploit. Novel defenses against such attacks are correspondingly unscripted, as they must be improvised in response to the specific unscripted features and re-scripting involved in an attack. In consequence, cybersecurity attacks are always uncertain events: attackers can never be certain when re-scripting will be successful, and defenders can never be certain when or where to expect an attack, as unscripted features are difficult to know until they are exploited.

Scripts in Practice

Information security teams occupy an unenviable position. Their work to secure computing infrastructures is often seen as a managerial function within organizations, with little account of the complexity of adversarial relationships, uncertainty, and instability inherent in the practice of information security. This should come as no small surprise given Star's (1999) observation that infrastructure—such as the infrastructural work of cybersecurity—is a taken-for-granted aspect of everyday life, only becoming visible when it fails. Yet for those who maintain infrastructure, anticipating failure of the systems under their care is integral to everyday life, with their

work devoted to ensuring that the user experience of infrastructure—the appearance of stable scripts—remains uninterrupted. The work of information security teams becomes visible and held to account only as users' scripts are destabilized when computing infrastructure is compromised by an attacker.

In focusing on stability, scripts have been critiqued for a lack of attention to breakdown and repair (Jarzabkowski and Pinch 2013), such as the instabilities encountered in the everyday work of information security teams. Indeed, Cetina (2001) encourages attention to breakdown and repair as being normal—rather than aberrant—conditions of "objectual practice" with technologies, requiring ongoing improvisation. Viewed in this way, it becomes essential to examine the spatial and temporal composition of practices of repair (Jackson 2016; Orr 1996) that keep computing infrastructures functioning. In conceptualizing cybersecurity, it is essential to move beyond repair to examine vulnerabilities, not just as failures needing repair but as active interventions by adversaries and cybersecurity engineers in crafting and responding to vulnerabilities (Spencer 2021). These issues are integral to cybersecurity, as Slayton and Clarke (2020) illustrate in their history of the emergence of computer security incident response teams.

Scripts and practices are two sides of the same coin. Scripts draw attention to materiality, needing to arrive at the eventual stability of sociotechnical relations in order to function. Practices capture a sense of contingency, providing ways to reconfigure and improvise sociotechnical relations in response to instability. Both are essential to my analysis, in which I examine, on the one hand, the causes and consequences of unstable scripts and, on the other hand, the contingent practices that evolve to deal with these instabilities. Given the adversarial relationships and uncertainty that define cybersecurity, the work of cybersecurity cannot help but be contingent, proceeding through necessarily improvised *unscripted practices* that function in relation to unstable scripts.

Methodology

The research for this project was conducted over the course of a year with information security teams at five university campuses in the United States. I spent approximately one month embedded with the information security team at each campus but remained in conversation with these teams through further visits. My research at each site was conducted with permission from the Chief Information Security Officer (CISO) who led the information security team at each campus. I began each of the five engagements with

a presentation to the information security team on my prior work, and the research I planned to conduct in my time with them. This gave the team a chance to get to know me and gave me the opportunity to address any questions or concerns they might have. As each campus presented a distinct set of problems, I conducted my research as a multisited ethnography (Marcus 1995), in which I followed people, things, stories, and conflicts across campuses through interviews and participant observation with information security teams as well as with the campus information technology staff and leadership. This approach afforded me the opportunity to understand the computing infrastructure at each campus, and the complex organizational structures and histories of interaction that shaped these infrastructures. The work I present here is relational, rather than comparative, as I focus on the broader patterns that became evident through my research to inform my critique of scripts.

At each campus, I was granted a desk in the same area as the information security team and was invited to attend their internal meetings, as well as their meetings with information technology staff across the campus. With permission, I shadowed members of each information security team as they went about their daily work. As I built relationships at each campus, I was invited to social gatherings of the information security teams, as much as to work meetings. At the conclusion of my time at each campus, I made a closing presentation to the information security team, in which I outlined my preliminary findings. I saw this as a means of accountability to offer any insights I gathered to the information security teams while giving them an opportunity to discuss and critique my research. In doing so, I followed Lave's (2011) admonition to be an apprentice both in my own ethnographic practice and in relation to those who I studied, creating spaces for reflection and ongoing engagement that are essential to critical ethnographic practice.

Incident Management in Three Views

"Management" calls forth an image of predictable, repeatable processes, of a world brought under control. "Incident" implies exception and irregularity in the seemingly smooth contours of the managed world. How are we to reconcile this opposition when understanding cybersecurity incident management?

In this section, I offer three linked perspectives from my fieldwork to examine the unscripted practices through which cybersecurity incident management proceeds. I begin by illustrating how cybersecurity concerns almost invariably overflow the expectations of stability in management and

scripts. I then examine how uncertainty is managed to account for stable experiences of user scripts in computing systems, even while these systems may be under threat. Finally, I study how cybersecurity depends upon improvised knowledge networks, which cannot be created or controlled by management. By presenting these three perspectives on incident management, I show how improvisation through unscripted practices is a necessary response to integrate uncertainty, adversarial relationships, and instability in cybersecurity into sociotechnical order.

Overflowing Scripts

"We receive over 5,000 incident reports every day." I'm walking to lunch with the CISO of a large university campus. He made this remark with a tone that was part boastful, part resigned, as though to say: "Look at how many incident reports we have! And, with this many incident reports, what are we to do?" The incident reports originate from the campus' intrusion detection system (IDS), a technology provided by a third-party vendor, which constantly analyses the campus computing infrastructure for signs of attacks. The vendor gathers threat intelligence from across their clients and from their own primary research, identifying signatures of attacks such as malicious domain names and IP addresses, suspicious patterns in data traffic, or observable indicators in installed software that mark a system as being possibly compromised. These signatures are compared against observations made within the campus computing infrastructure to identify potential attacks. The IDS plays an invaluable role in the campus' information security capabilities. In theory, the IDS offers a straightforward script for managing incidents, reporting them to the information security team who need only deal with remediation. In practice, incidents overflow this script for both the IDS vendor and the information security team—a consequence of the sheer volume of incident reports and the novelty of attacks.

The campus serves more than 40,000 students, with a complex computing infrastructure to support diverse academic units spanning physical sciences, engineering, medicine, arts and humanities, social sciences, and more—many of which manage their own computing requirements. The information security team has the responsibility of providing centralized support for securing these diverse systems across the campus. The CISO recounted the challenges that the IDS vendor faced in this complex environment: "We were told the day they turned us on we were their noisiest customer in the world." He added wryly that the campus is effectively a honeypot (a system intended to attract attacks for research purposes), making it a source of

threat intelligence for their IDS vendor as much as a customer seeking protection.

Not every incident report marks a real attack. Some are false positives, detecting legitimate uses and behaviors in campus computing systems. More dangerous are false negatives, which categorize an incident as normal behavior, or report an incident as being of lower severity than it actually is. To the extent possible, all incident reports need investigation to separate false positives from real incidents, to analyze the actual severity of incidents, and to identify the affected systems. Although the IDS provided useful information on potential threats, only the campus information security team possessed the knowledge of computing infrastructure to appropriately evaluate each incident report, as prior studies have recognized (Goodall, Lutters, and Komlodi 2009; Ben-Asher and Gonzalez 2015; Alahmadi, Axon, and Martinovic 2022). A manager on the team reflected on the difficulties they faced:

> Some of the stuff that they've told us is low, is actually high; and some of the stuff that they've told us is medium or high, is probably just low. We receive a lot of false positives, and also false negatives, not a lot, but it has happened that we've had a false negative. I mean, the question is, do they understand our infrastructure? You can only escalate something into a certain severity if you understand infrastructure at the same time.

The information security team numbered eighteen people at the time of my visit, of whom about half were concerned with incident management. They were supplemented by several undergraduate student interns who worked as entry-level incident responders, responsible for managing the large volume of low-level incidents. But with more than 5,000 incident reports daily in a complex campus computing infrastructure, it is a near impossible task to give each incident report the level of attention it deserves, even with a well-resourced information security team. A senior analyst on the team related the difficulties they faced in managing this volume of incident reports:

> Absolutely, it's a bandwidth issue. It's just because we're trying to, for my team at least, react to all the alerts that are coming in constantly, and at the same time, push new technologies out, so that we can hopefully limit those incidents that are coming in. Pretty much every week we have a major security incident where we have to go into forensics and spend time, and actually do analysis. When you have that type of resource usage, it's hard to

> even implement new technology . . . . I have no idea what to expect every day. The first two or three hours of my job is going to be handling these few regular tasks, but the rest of the day I leave open because everything and anything will come by and you just kind of have to take it and go with it.

With this degree of uncertainty and volume of work, I wondered how the team kept up with the constantly evolving nature of threats, as adversaries develop new kinds of attacks. The analyst's response was telling, illustrating how integral learning on the job is to her practice in the constant improvisation necessary to respond to novel attacks:

> I used to go to classes, go to conferences all the time, I used to every day read a new article and get a better understanding. Here, you see those things, this is kind of the birthplace for a lot of zero days . . . we discover a lot of alerts and security threats that haven't even really been disclosed by vendors or have just been disclosed like an hour ago, and we're already seeing it. I used to joke that our campus was like a cesspool and you see new things breeding all the time, and you get new germs every single day and new viruses. I don't have the time or the bandwidth to learn new things outside of work. Thankfully, work has brought them to me.

The problem the campus information security team faces isn't that of ensuring a stable script within the actor network of the IDS and other related sociotechnical systems. Rather, their challenges arise from the sheer volume of ongoing attacks by adversaries and the uncertainty of how, when, or where attacks might arrive in the campus computing infrastructure. The resulting scripts are profoundly unstable, with the volume and novelty of attacks overflowing any expectation or hope of predictability in both scripts and the management of cybersecurity. Resistance to scripts—de-inscription—is often accounted for as differing interpretations of scripts, which I have termed interpretive instability. By contrast, I note that the scripts of cybersecurity carry within themselves the potential for de-inscription in which all actors—the campus information security team, the IDS vendor, and even attackers—find themselves forced to deal with the constant uncertainty inherent in adversarial instability.

Renegotiating Relations

I started my research at a much smaller campus, with an information security team of only five people. I was sitting in on a weekly team meeting when one of the analysts reported a problem he'd been working on with the

payment systems operated by the campus dining services. Given the sensitive nature of the credit card information handled by these systems, I anticipated it might be a serious issue, calling for a substantial response. As my transcript of the meeting illustrates, I couldn't have been more wrong.

B: I've been dealing with an issue on the cellular modems on the payment card interfaces.
J: What's the exposure of these systems?
B: They're confined, and no sensitive data is involved. All the modems do is set up an IPSec VPN.
C: The [cellphone company] consultant didn't say what it is exactly, but I think it's a Mirai-type infection. The only danger is of excessive traffic.
B: It's still a low risk, as it's unlikely any data will be compromised. They'll be patching the systems with a firmware update.
C: What about system vulnerabilities, like default passwords, or a back-door maintenance account?
B: These are locked down when the systems are configured.

As B notes in response to J's question, the problem is located in cellular modems responsible for setting up an encrypted connection—the IPSec VPN, a technology for secure network communications—to a payment gateway. Although the modems channel credit card information for payments, they don't carry sensitive user information that could facilitate fraud. The modems are "confined" with no connectivity to the larger campus network, eliminating the possibility that they might be used to stage compromises of other computing systems across the campus. The modems are not owned or operated by the campus but rather by the cellphone company, which provides connectivity for the payment systems. In consequence, B and C needed to contact the cellphone company support to help diagnose and address the issue. As they discovered, the modems were compromised by a "Mirai-type infection." Mirai infects Internet of Things (IoT) devices, re-scripting them to make them part of a botnet used to mount distributed denial of service (DDoS) attacks on unwitting targets. Infected devices continue to function normally, even while using their network connectivity to collectively overload targets with requests. Several variants of Mirai have emerged over the years, as the original Mirai has been modified to adapt to countermeasures. The use of default passwords and unsecured maintenance accounts on devices are among the most common vectors for Mirai-type infections, which is why C asked about these, to work out how the modems

were infected in the first place. B's response that these are locked down indicates that the vector of infection was likely a vulnerability in the modem firmware—an unscripted feature—rather than a configuration issue. This is probably why they expected the cellphone company to issue a firmware update in response to this problem.

When B joined the team, he was made responsible for managing the security of payment systems across the campus, as he had past experience in this area. However, B is less confident in his technical skills than many other members of the team, having begun his working life as a history teacher and transitioning to information security only later in life. B relies on the team for their broader expertise in information security—such as C's knowledge of Mirai—even as the team relies on him for his knowledge of payment systems and of the security audit requirements that payment processors demand for the operation of these systems.

The collaborative response I witnessed was by no means unusual, illustrating how sociotechnical relations are constantly renegotiated in the unscripted practices of cybersecurity. The team renegotiated relations with each other, with the cellphone company consultant, and with the infected cellular modems, to respond to the specific issue at hand, sharing and building on their prior knowledge (Ahrend, Jirotka, and Jones 2016). As I realized, unscripted practices are a necessary source of stability both for user scripts (e.g., deciding to keep payment systems running while infected) and for information security teams. By providing the freedom of action necessary to respond to uncertainty, unscripted practices provide the room for collective sense-making and coordination to construct bespoke responses to newly discovered attacks and vulnerabilities. This is not a matter of eliminating or reducing uncertainty, but rather of integrating uncertainty and adversarial relationships into the social practice and organizational form of the information security team.

Malleable Knowledge

As I came to understand cybersecurity practices as unscripted, I was faced with a problem: if the knowledge required for these practices is constantly evolving in response to new kinds of attacks, how is this knowledge produced? Part of the answer to this question lies in individuals' and teams' capacity to learn on the job to improvise responses to attacks and use third-party threat analysis in tools such as the IDS. However, given the intricacies of sophisticated attacks, and the global range of attackers, no single team, individual, or tool can produce all the knowledge needed for defense.

In discussing this issue with incident response personnel across the teams I studied, it became evident that they each drew from personal knowledge networks built up over the course of their career. An analyst related how he came to form the relationships through which he draws knowledge:

> Starting probably in 2013 at my last job, I would post up—I'm not sure if you're familiar with Angler and Rig exploit kit, if you've ever heard of those exploit kits—so I would see that traffic come through on my last job on the network, and I would post it up on Twitter. "Hey, I saw this traffic." One of the individuals, we chatted quite a bit, because he did a lot of research. . . . But I think I just got looped in on some other Twitter groups and somehow I got invited to this Slack channel where a lot of us do research on exploit kits, and so we share some intel with each other. A lot of stuff I see that we share and talk about on our Slack channel, I see here a lot too. There's a quite a few other people that are in there. People from Cisco, someone from Malware Bytes, a couple other people. I mean, it's all just independent research. That's where I mostly get my stuff.

The analyst told me how he'd never met any of the people from the Slack channel in person. These were entirely online relationships, which he gained access to by sharing his analysis of attacks, eventually being invited to the closed group of knowledgeable peers in the Slack channel on the strength of his reputation. Considering the sensitivity of the information being shared, closed groups are essential to the production and circulation of cybersecurity knowledge (Mathew and Cheshire 2018).

Knowledge networks have material as well as social bases, since analysts need safe computing systems in which to study malware involved in attacks. It can be difficult to allow for such systems within campuses, as there's always a fear that malware might escape safeguards to attack the campus computing infrastructure. Some of the teams I worked with resolved this issue by building custom computing systems, on which all network connectivity was disabled, to minimize the risk that the malware being studied on these systems might spread to other computing systems on campus. Others used personal secure computing environments for this purpose. There was no single solution to this problem of building a safe environment for studying malware, as each team or individual improvised approaches suitable to their particular situations. An analyst walked me through his process for studying malware:

> Sometimes, I'll get stuck on an alert, which I'm not familiar with, so it'll require some research, some reading. I have a lab box at home that's an empty

> network, sometimes I'll log into, and I'll download the piece of malware and I'll do some just quick low-level static analysis. I'll just dump the strings, check the hashes, I'll upload it to Hybrid Analysis, which is a dynamic analysis engine on the internet. I'll run that. I mean, it really depends on what's coming through.

Since he couldn't operate a secure environment for malware analysis on campus, the analyst maintained one at home, supplementing this with the use of free online tools such as Hybrid Analysis. Although he had devised his own process for the initial analysis of malware, the steps involved in more sophisticated analysis depended entirely upon the constantly changing specifics of "what's coming through."

"Once technical objects are stabilized, they become instruments of knowledge," argues Akrich (1992, 221). But how are we to handle knowledge in unstable objects with unstable scripts? The knowledge required to engage with unstable scripts is itself unstable. It must remain malleable, retaining the potential for improvisation to recognize and respond to novel vulnerabilities and attacks. Just as attackers construct new knowledge in discovering unscripted features and exploiting them through re-scripting, information security engineers construct new knowledge in their analysis of, and response to, attacks. The resulting knowledge networks cannot be constrained by management within organizational boundaries, as engineers necessarily draw on broader sociotechnical relations to reason about the global threat environment in which they operate (Goodall, Lutters, and Komlodi 2004; Kocksch et al. 2018).

Unscripted Practices

Scripts offer powerful tools for analyzing designer–user relationships mediated by technical objects. However, their essential weakness lies in the emphasis upon stability. Nowhere is this weakness more apparent than in cybersecurity, where instability in scripts is not only a matter of repair and maintenance (Jarzabkowski and Pinch 2013) but is equally concerned with the adversarial instability involved in handling attacks by adversaries who actively seek to disrupt computing systems. This requires consideration of adversarial relationships founded upon irreconcilable disagreement and diametrically opposed interests in the analysis of scripts, just as much as consideration of collaborative relationships that might lead to a negotiated agreement or of multistable systems (Lannge and Borg 2021) in which multiple scripts coexist without disrupting one another.

Adversarial oppositions are sustained by the material affordances of computing which intentionally offer resistance to stability, allowing computing systems to be turned to arbitrary purposes through programming and reconfiguration—and also opening them up to re-scripting by exploiting vulnerabilities. The results, as we have seen, are unstable scripts that depend upon unscripted practices, illustrating the limits of stable scripts for analysis and showing how practice can help to address these limits. For example, the case of the compromised modem shows how networks of relationships (in the script of the payment system, and in the information security team) require ongoing renegotiation in practice to respond to attacks.

Examining changing relations of practice can also help explain how knowledge of cybersecurity is constructed in relation to unstable scripts—a key problem for the field. Knowledge may be formed in response to particular incidents (Spencer 2021), but it is maintained in situated sociotechnical relations of practice: through on-the-job experiences of previously unknown vulnerabilities and attacks, through ongoing collaboration in private groups with peers, and in the materiality of research infrastructures that analysts use within and across organizational boundaries (such as an IDS or a personal lab system).

As discussion of the IDS illustrates, cybersecurity concerns invariably overflow attempts at creating stable scripts and management. Yet unstable scripts need not imply an unstable user experience of computing systems. Unscripted practices respond to unstable scripts by offering contingency for the improvisation necessary to integrate uncertainty and adversarial relationships into the social practices and scripts of cybersecurity. In illustrating the limits of stable scripts, cybersecurity forces us to consider how instability might be a normal condition for scripts, rather than a transient moment on the path to stability.

Akrich's conception of scripts continues to be an invaluable tool for analyzing sociotechnical systems. However, the case of cybersecurity shows how attention must sometimes be turned from anticipating negotiated stability in designer–user relationships toward anticipating uncertainty in adversarial attacker–defender relationships—the proximate cause of unstable scripts in cybersecurity. Unstable scripts call to attention conditions in which subversion is an everyday occurrence; in which uncertainty, adversarial relationships, and instability are integral to sociotechnical order; and to which the only response can be improvisation, readily apparent in the unscripted practices of cybersecurity.

Acknowledgments

I would like to thank the two anonymous reviewers and Luca Vigano for their comments, which were invaluable in clarifying my arguments. This article would not have been possible without the intellectual and logistical support that the editors of this special issue—Annalisa Pelizza and Claudia Aradau—provided over many extended conversations.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Ashwin Jacob Mathew https://orcid.org/0000-0002-5124-3622

References

Abend, Pablo, and Benjamin Beil. 2016. “Editors of Play: The Scripts and Practices of Co-creativity in Minecraft and LittleBigPlanet.” *Transactions of the Digital Games Research Association* 2 (3): 55-72. doi: 10.26503/todigra.v2i3.51.

Ahrend, Jan M., Marina Jirotka, and Kevin Jones. 2016. “On the Collaborative Practices of Cyber Threat Intelligence Analysts to Develop and Utilize Tacit Threat and Defence Knowledge.” 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1-10, IEEE, London, UK. doi: 10.1109/CyberSA.2016.7503279.

Akrich, Madeleine. 1992. “The De-Scription of Technical Objects.” In *Shaping Technology/Building Society*, edited by Wiebe Bijker and John Law, 205-24. Cambridge, MA, USA: MIT Press.

Akrich, Madeleine, Michel Callon, and Bruno Latour. 2011. “The Key to Success in Innovation Part I: The Art of Interessement.” *International Journal of Innovation Management* 6 (2): 187-206. doi: 10.1142/S1363919602000550.

Alahmadi, Bushra A, Louise Axon, and Ivan Martinovic. 2022. “99% False Positives: A Qualitative Study of SOC Analysts’ Perspectives on Security Alarms.”. In *Proceedings of the 31st USENIX Security Symposium*, 2783-2800. Boston, MA, USA.

Bambauer, Derek E. 2014. “Ghost in the Network.” *University of Pennsylvania Law Review* 162 (5): 1011-91.

Ben-Asher, Noam, and Cleotilde Gonzalez. 2015. "Effects of Cyber Security Knowledge on Attack Detection." *Computers in Human Behavior* 48: 51-61. doi: 10.1016/j.chb.2015.01.039.

Bilge, Leyla, and Tudor Dumitraş. 2012. "Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World." In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, edited by Ting Yu, George Danezis, and Virgil Gligor, 833-44. CCS '12. New York: Association for Computing Machinery. doi: 10.1145/2382196.2382284.

Carey, Benjamin. 2016. "Artefact 'Scripts' and the Performer-developer." *Leonardo* 49 (1): 74-75. doi: 10.1162/LEON_a_01117.

Coppens, Paulien, Carina Veeckman, and Laurence Claeys. 2015. "Privacy in Location-based Social Networks: Privacy Scripts & User Practices." *Journal of Location Based Services* 9 (1): 1-15. doi: 10.1080/17489725.2015.1017015.

Esfahani, Naghmeh Nouri, and Victoria Carrington. 2015. "(Re)Scripting Barbie: Postphenomenology and Everyday Artefacts." In *Phenomenology of Youth Cultures and Globalization*, edited by Stuart R. Poyntz and Jacqueline Kennelly, 116-31. New York: Routledge.

Feenberg, Andrew. 2019. "The Internet as Network, World, Co-construction, and Mode of Governance." *The Information Society* 35 (4): 229-43. doi: 10.1080/01972243.2019.1617211.

Gartzke, Erik, and Jon R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24 (2): 316-48. doi: 10.1080/09636412.2015.1038188.

Gartzke, Erik, and Jon R. Lindsay. 2017. "Thermonuclear Cyberwar." *Journal of Cybersecurity* 3 (1): 37-48. doi: 10.1093/cybsec/tyw017.

Goodall, John R., Wayne G. Lutters, and Anita Komlodi. 2004. "I Know My Network: Collaboration and Expertise in Intrusion Detection." In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, edited by Jim Herbsleb and Gary Olson, 342-45. Chicago, IL: ACM. doi: 10.1145/1031607.1031663.

Goodall, John R., Wayne G. Lutters, and Anita Komlodi. 2009. "Developing Expertise for Network Intrusion Detection." *Information Technology & People* 22 (2): 92-108. doi: 10.1108/09593840910962186.

Hedström, Karin, Gurpreet Dhillon, and Fredrik Karlsson. 2010. "Using Actor Network Theory to Understand Information Security Management." In *Security and Privacy—Silver Linings in the Cloud*, Vol. 330, edited by Kai Rannenberg, Vijay Varadharajan, and Christian Weber, 43-54. IFIP Advances in Information and Communication Technology. Berlin, Germany: Springer Berlin Heidelberg. doi: 10.1007/978-3-642-15257-3_5.

Igelsböck, Judith. 2016. "Engaging with the Concept of the 'Script' in Industrial Innovation Studies—or How Retro–ANT Is Perfect but Not 'Enough.'" In *Proceedings of the 6th STS Italia Conference*, 435-46. Trento, Italy. http://www.stsitalia.org/wp-content/uploads/2019/02/STS-Trento-Proceedings.pdf.

Jackson, Steven J. 2016. "Speed, Time, Infrastructure: Temporalities of Breakdown, Maintenance, and Repair." In *The Sociology of Speed: Digital, Organizational, and Social Temporalities*, edited by Judy Wajcman and Nigel Dodd, 169-86. Oxford, UK: Oxford University Press.

Jarzabkowski, Paula, and Trevor Pinch. 2013. "Sociomateriality Is 'the New Black': Accomplishing Repurposing, Reinscripting and Repairing in Context." *M@n@gement* 16 (5): 579-92.

Jovanovic, Boyan, and Peter L. Rousseau. 2005. "Chapter 18—General Purpose Technologies." In *Handbook of Economic Growth*, Vol. 1, edited by Philippe Aghion and Steven N. Durlauf, 1181-224. Elsevier. doi: 10.1016/S1574-0684(05)01018-X.

Karlsson, Fredrik, and Karin Hedström. 2014. "End User Development and Information Security Culture." In *Human Aspects of Information Security, Privacy, and Trust*, Vol. 8533, edited by Theo Tryfonas and Ioannis Askoxylakis, 246-57. Lecture Notes in Computer Science. Cham, Switzerland: Springer International. doi: 10.1007/978-3-319-07620-1_22.

Knorr Cetina, Karin. 2001. "Objectual Practice." In *The Practice Turn in Contemporary Theory*, edited by Karin Knorr Cetina, Theodore R. Schatzki, and Eike von Savigny, 185-97. London, UK and New York, NY, USA: Routledge.

Kocksch, Laura, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. "Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices." In *Proceedings of the ACM on Human-computer Interaction*, Vol. 2, edited by Karrie Karahalios, Andrés Monroy-Hernández, Airi Lampinen, and Geraldine Fitzpatrick, 1-20. New York: ACM. doi: 10.1145/3274361.

Lannge, Ditte Bendix, and Søren Risdal Borg. 2021. "Multistable Infrastructure: The Scripted and Unscripted Performance of a Funtionalist Pathway." In *Postphenomenology and Architecture: Human Technology Relations in the Built Environment*, edited by Lars Botin and Inger Berling Hyams, 19-43. London, UK: Lexington Books.

Latour, Bruno. 1990. "Technology Is Society Made Durable." *Sociological Review* 38 (S1): 103-31.

Lave, Jean. 2011. *Apprenticeship in Critical Ethnographic Practice*. London, UK: University of Chicago Press.

Marcus, George E. 1995. "Ethnography in/of the World System: The Emergence of Multi-sited Ethnography." *Annual Review of Anthropology* 24 (01): 95-117.

Mathew, Ashwin Jacob, and Coye Cheshire. 2018. "A Fragmented Whole: Cooperation and Learning in the Practice of Information Security." Technical Report. UC Berkeley Center for Long-Term Cybersecurity and Packet Clearing House. Accessed March 20, 2024. https://www.pch.net/resources/Papers/A_Fragmented_Whole/.

Michael, Mike. 1996. "Technologies and Tantrums: Hybrids out of Control in the Case of Road Rage." Presented at the "Signatures of Knowledge Societies" Joint 4S/EASST Conference, University of Bielefeld, Bielefeld, Germany.

Mulligan, Deirdre K., and Daniel S. Griffin. 2018. "Rescripting Search to Respect the Right to Truth." *Georgetown Law Technology Review* 2 (2): 557-84.

Orr, Julian E. 1996. *Talking About Machines: An Ethnography of a Modern Job*. Ithaca, NY: Cornell University Press.

Pelizza, Annalisa. 2021. "Towards a Sociomaterial Approach to Inter-organizational Boundaries: How Information Systems Elicit Relevant Knowledge in Government Outsourcing." *Journal of Information Technology* 36 (2): 94-108. doi: 10.1177/0268396220934490.

Pieters, Wolter. 2011. "Representing Humans in System Security Models: An Actor-network Approach." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2 (1): 75-92.

Pieters, Wolter, Julian Padget, Francien Dechesne, Virginia Dignum, and Huib Aldewereld. 2013. "Obligations to Enforce Prohibitions: On the Adequacy of Security Policies." In *Proceedings of the 6th International Conference on Security of Information and Networks—SIN '13*, edited by Atilla Elçi, Manoj Singh Gaur, Mehmet A. Orgun, and Oleg B. Makarevich, 54-61. Aksaray, Turkey: ACM Press. doi: 10.1145/2523514.2523526.

Plasil, Tanja. 2020. "'Best Before, Often Good After': Re-scripting the Date Label of Food in Norway." *Nordic Journal of Science and Technology Studies* 8 (1): 16-26. doi: 10.5324/njsts.v8i1.3396.

Pollock, Neil. 2005. "When Is a Work-around? Conflict and Negotiation in Computer Systems Development." *Science, Technology, & Human Values* 30 (4): 496-514. doi: 10.1177/0162243905276501.

Rasmussen, Majken Kirkegaard, and Marianne Graves Petersen. 2011. "Re-scripting Interactive Artefacts with Feminine Values." In *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces—DPPI '11*, edited by Alessandro Deserti, Francesco Zurlo, and Francesca Rizzo, 1-8. Milano, Italy: ACM Press. doi: 10.1145/2347504.2347515.

Rosenberger, Robert. 2014. "Multistability and the Agency of Mundane Artifacts: From Speed Bumps to Subway Benches." *Human Studies* 37 (3): 369-92. doi: 10.1007/s10746-014-9317-1.

Samonas, Spyridon, and David Coss. 2014. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security* 10 (3): 21-45.

Slayton, Rebecca. 2021. "Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties." *Science, Technology, & Human Values* 46 (1): 81-111. doi: 10.1177/0162243919901159.

Slayton, Rebecca, and Brian Clarke. 2020. "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005." *Technology and Culture* 61 (1): 173-206. doi: 10.1353/tech.2020.0036.

Spencer, Matthew. 2021. "Creative Malfunction: Finding Fault with Rowhammer." *Computational Culture*, no. 8 (July). Accessed March 20, 2024. http://computationalculture.net/creative-malfunction-finding-fault-with-rowhammer/.

Star, Susan Leigh. 1999. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43 (3): 377-91. doi: 10.1177/00027649921955326.

Von Schnitzler, Antina. 2013. "Traveling Technologies: Infrastructure, Ethical Regimes, and the Materiality of Politics in South Africa." *Cultural Anthropology* 28 (4): 670-93. doi: 10.1111/cuan.12032.

Ward, Matt, and Alex Wilkie. 2008. "Made in Criticalland." In *Proceedings of the 2008 Annual Conference of the Design History Society (UK)*, 118-23. Falmouth, UK: Design History Society.

Wilkie, Alex. 2020. "How Well Does ANT Equip Designers for Socio-material Speculations?" In *The Routledge Companion to Actor-network Theory*, edited by Ignacio Farias, Celia Roberts, and Anders Blok, 389-99. London, UK; New York: Routledge, Taylor & Francis Group.

Author Biography

Ashwin Jacob Mathew is a Lecturer in Global Digital Cultures in the Department of Digital Humanities at King's College London. He is an ethnographer of internet infrastructure, focusing on the practices of the technical communities who build and operate the global internet, including network administrators and cybersecurity engineers.