Contemporary Security Policy

ISSN: 1352-3260 (Print) 1743-8764 (Online) Journal homepage: https://www.tandfonline.com/loi/fcsp20

Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet

Clare Stevens

To cite this article: Clare Stevens (2020) Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet, Contemporary Security Policy, 41:1, 129-152, DOI: 10.1080/13523260.2019.1675258

To link to this article: https://doi.org/10.1080/13523260.2019.1675258

Published online: 15 Oct 2019.

CONTEMPORARY SECURITY POLICY
2020, VOL. 41, NO. 1, 129–152
https://doi.org/10.1080/13523260.2019.1675258

Routledge
Taylor & Francis Group

Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet

Clare Stevens

School of Sociology, Politics and International Studies, University of Bristol, Bristol, UK

ABSTRACT
This is an article about how cybersecurity gets "made," with a focus on the role of commercial computer security firms in generating knowledge in matters of international cybersecurity. The argument is two-fold. Firstly, malware may be an intangible artefact in some ways, but its success and its interpretation as malware is deeply interwoven in social, technical, and material alliances. Secondly, a materialist-minded examination of Symantec's Stuxnet reports will demonstrate the politically situated nature of how cybersecurity expertise emerges. The article finds that Symantec's work was not a-political or neutrally-technical: Their experts made profoundly political choices in their analyses. By showing the processes that go into making cybersecurity, the article contributes to a widening and deepening of debates about what is at stake in cybersecurity knowledge and practices.

KEYWORDS Intangible artifacts; cybersecurity; security studies; materiality; Stuxnet

In June 2010, a piece of malicious computer coding was discovered and described by specialists, dealing with computer software security, as a "sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion" (Farwell & Rohozinski, 2011, p. 24). According to the discovering specialists, infections were most predominant in Iran, suggesting this was the target (Falliere, O'Murchu, & Chien, 2011). Beginning in June of 2010, the computer security organization Symantec began publishing a series of blog entries and reports through their website concerning a piece of malware that became known as "Stuxnet." Over the course of the following eighteen months these reports documented the findings from the company's efforts at reverse engineering the malware.

CONTACT Clare Stevens ✉ cs13554@bristol.ac.uk School of Sociology, Politics and International Studies, University of Bristol, 11 Priory Rd, Bristol, BS8 1TU, UK

Though their research and publication efforts were the most extensive, Symantec were by no means the only source of information about the malware and its "family" of associated malware incidents. Antivirus (AV) companies such as Kaspersky, ESET and F-Secure as well as a whole host of individual researchers contributed their own findings to the gradual accretion of knowledge about Stuxnet. Technical analyses of other malware incidents have since linked other events to Stuxnet, incidents that shared modules, coding, or behaviors with this malware, such as "Duqu," "Flame," and "Gauss." Despite the time that has passed since Stuxnet's discovery, these incidents are still the subject of research and publicity in 2019: Another company, Chronicle (2019), recently described their discovery of new elements of the Stuxnet code with the use of "modern techniques" for malware analysis.

Symantec's descriptions of the Stuxnet coding was one of the earliest examples of its kind: a technical malware report entangled in the politics of nuclear proliferation, diplomacy, international law, and the mechanisms of global cybersecurity governance. Though initial Stuxnet infections occurred a decade ago this year, Symantec's reports are a landmark occurrence in the emergence of commercial cybersecurity expertise in the context of strategic state cyber operations. Until this point, market-oriented entities such as Symantec had not taken such a forthright role in materializing cybersecurity knowledge on the international stage. As one of the researchers later observed, "We really weren't cyberwar-trained until Stuxnet," (O'Murchu, as cited in Jackson Higgins, 2019). And yet, the role of commercial computer security firms[1] in generating knowledge in international "cyber" dynamics are still largely understudied.

This article is about how cybersecurity gets "made." Drawing on the insights of "materially minded" security studies, I argue that the success of complex malware as well as the political legitimacy of commercial firms as security actors requires the mobilization of multiple alliances. These can be conceptual alliances, based on ideas such as the role of the firm in protecting customers, or ideas about the rightful place of the state as security provider (such as "public" versus "private" security). They can be material, consisting of centrifuges, buildings, hardware, industrial control systems, HE6 particles. They may be social links, including the programmers, the "hackers," the operators, the unwitting carrier or vector. It might be textual, such as the coverage, news reports, publicity to make the reports available. Malware may be an intangible artefact in some ways, but in other ways its success and its interpretation as malware is deeply interwoven with social, technical and material alliances.

This article will demonstrate that Symantec's efforts are illustrative of a dynamic identified by Balzacq and Dunn Cavelty (2016), one that they have argued is an important but under-appreciated element in the cybersecurity literature. Focusing on the speech-acts of visible political actors has meant that "the preceding and preparatory practices of actors that are not as easily visible, also outside of governments" have been overlooked in the literature, missing out on the ways that "the material 'realities' of computer disruptions" are interpreted in technical communities which "then serve as a basis for political action" (Balzacq & Dunn Cavelty, 2016, p. 5). Reports such as Symantec's are an important constitutive element in wider practices of hardening facts about threats. Such reports can thus help us trace how some incidents attain political salience and serve as the basis for wider political action and policy. This is not just about technical aptitude and seeking out the most "accurate" or "correct" technical accounts. Instead this article argues that we need to address how these same incidents can be reported in very different ways and that these are not purely technical reports: They are loaded with political, instrumental, and strategic choices**.** There are also a range of commercial incentives at work.

Given the centrality of technology to practices of cybersecurity, this highlights the need for a different kind of approach, one that can recognize technology's productive role in such arrangements. Cybersecurity is simultaneously a technical and cultural formulation, with important ramifications for the political responses that arise as a result. However, the processes involved in the production of cybersecurity knowledge have received relatively little scholarly attention. Technical reports such as Symantec's offer a prime resource for understanding how malware is described, but they also give researchers an insight into the "material context in which certain security practices become possible" (Lundborg & Vaughan-Williams, 2015, p. 15). After all, cybersecurity "is a type of security that enfolds in and through cyberspace, so that the making and practice of cyber-security is at all times constrained and enabled by this environment" (Balzacq & Dunn Cavelty, 2016, p. 4). The reports of companies such as Symantec and Kaspersky see them acting as representatives, translators and spokespersons for malware. As this article will draw out then, the interesting critical point is not to simply focus on how particular incidents came to pass at the technical level, but rather to understand why particular configurations of otherwise silent or invisible actors and computers become visible at particular times and places, and to ask how the intangible or invisible workings of these technologies get "made thingy" (Rankin, 2014, p. 664) at specific moments.

Recent scholarship has underscored the potential utility of studying the emergent practices around cybersecurity and transnational technologies using insights gleaned from the Science and Technology Studies (STS) literature (Collier, 2018; De Goede, 2018; Dunn Cavelty, 2018; Stevens, 2018), while scholars such as Kearns (2016, 2017), Van Veeren (2014) and Walters (Best & Walters, 2013; Walters, 2014) vividly illustrate the kinds of material traces that can be left in the public sphere and the kinds of materialist-minded analyses that we can productively undertake as a result. However, while these scholars offer rich conceptualizations and methodological approaches for studying such opaque security contexts, these insights have yet to be developed in the context of (commercial) cybersecurity practices. With these insights in mind, the article will contribute to the productive conversation between security studies and STS by showing how the kind of materialist analysis proposed can help researchers move beyond acts of rhetoric to examine the “material realities” that precede and shape threat perceptions and cyber politics more broadly. By engaging with the role of things and materiality this approach will emphasize how cybersecurity and international security are subject to more than rhetorical securitization but emerge out of complex material-discursive practices (Aradau, 2010).

The article will proceed as follows. The discussion will begin by drawing out what is at stake in emergent cybersecurity practices, and the importance of analyzing the processes of its “making.” Here, the article will show how Symantec’s work was taken as a-political technical analysis as it was translated into wider “cybersecurity” discourses and reports. Then, following McCarthy’s (2018) call to theoretically “deepen” our understandings of the politics inherent in cybersecurity processes, the second section will map out an approach that can help us scrutinize these processes. Here the article will make a methodological argument about tracing “intangible artifacts.” Malware and coding are materials that exceed human capacities to sense or understand them, so that they do not present themselves to us in unmediated fashions: They require spokespersons, mediators, interpreters. This section will therefore outline a materialist-minded approach that can trace the situated and contingent alliances mobilized in reports such as Symantec’s, drawing on Latour’s (2005, 2007) and Walters’s (2014) discussion of “public assemblies.” The main part of the article will then be taken up with an empirical account of a specific site of emergent practices of knowledge production in the field of cybersecurity, and the dynamics between state and non-state actors. It will follow the processes as Symantec transform and translate fragments of the Stuxnet code into “things” and the alliances that they have to forge to make them meaningful. This will show how Symantec’s was not a-political or neutral technical work: They made profoundly political choices in their analyses. In conclusion, this empirical analysis will draw out the importance of recognizing that different readings of malware lead to different goods, or different policy implications. This article means to demonstrate that wider policy decisions about what is taken as good or acceptable practice are not down to matters of technical accuracy or proficiency alone.

How cybersecurity gets made

“Cybersecurity” signifies a multifarious range of technologies, processes, practices, and complex socio-technical arrangements, coagulating around this concern with security in and through cyberspace. What was once described simply as computer security, cybersecurity is no longer the remit only of private or corporate practitioners but has become a complex site of interaction between a very wide range of people, organizations and technologies, especially in statist discourses. This complex array of material and human interactions is thus captured by an heterogenous set of discourses and practices, sometimes with competing purposes and even contradictory underlying conceptualizations of the thing to be secured. Because it is gradually emerging with the growth and penetration of networked technologies, cybersecurity is therefore not a static set of discourses and practices. It is a work-in-progress, emergent along with the recursive interactions of communications technologies with their associated societal processes. There are many sites where cybersecurity appears and is "made" as a result, co-produced between a wide range of users, groups, institutions, laws, materials, protocols and practitioners (Balzacq & Dunn Cavelty, 2016). As critical security studies emphasize, "security is time and again 'in the making'" (Schouten, 2014, p. 25). The research and reports of commercial security actors such as Symantec are but one small facet of this messy emergent ecosystem.

However, the role of commercial cybersecurity firms and their technical reports has had relatively little academic attention.[2] Because so much of these networks and infrastructures are in private and corporate hands (estimates of around 90% in the United States for example), the private sector is hailed by the state as the "cornerstone" of cybersecurity strategies (Carr, 2016; White House, 2003, p. vii). To the extent that this complexity and breadth of actors in cybersecurity arrangements has been addressed in the literature, it has as mirrored this concern in official policy discourses, describing the role of commercial firms role within the idiom of "public-private partnerships" (Bossong & Wagner, 2016; Carr, 2016; Christensen & Petersen, 2017; Dunn-Cavelty & Suter, 2009). Yet there are distinctive features to the dynamics in cybersecurity which suggest that there are limitations to trying to understand the role of the commercial actors in cybersecurity through the framework of a PPP (Collier, 2018; McCarthy, 2018).

Cybersecurity is not something that was once the state's duty and which they subsequently delegated to commercial actors (Eichensehr, 2017). It is an issue that is emerging with the development and integration of information communication technologies with everyday life. Cybersecurity is therefore not just the privatization of a previously government roles, but the emergence of an entirely new kind of public good in which state-based and commercial actors are negotiating and sometimes even contesting the boundaries for their respective roles and responsibilities. In the context of broader trends in security governance, the PPP model thus has limitations to such a way of conceptualizing the relationships between state-based and commercial security rationales. In fact, the complex social, political, technical, and economic processes that are informing cybersecurity practices have led some scholars to argue that these processes exceed traditional framings of "public" and "private" (Collier, 2018). A further critical point emerges. Conceptual frameworks that start uncritically from this analytical distinction risk missing from their accounts some of the complex processes symptomatic of cybersecurity practices, whilst also uncritically reproducing those normative and political assumptions (McCarthy, 2018). These insights are salient starting points in the case of Symantec and other commercial firms.

In addition to their role as owners and operators of infrastructures and networks, the expertise of commercial actors is also a key resource as far as policymakers and advisers are concerned. In the case of Symantec's analysis of Stuxnet, their work formed an integral part of much of the media reportage and academic writing that followed the deployment of the malware and contributed to the narrative of "Stuxnet" as a geopolitical event. For example, the think-tank Institute for Science and International Security (ISIS) worked with Symantec to produce a series of reports regarding the technical details of Stuxnet and its intended target (Albright, Brannan, & Walrond, 2010; Albright & Stricker, 2010; ISIS, 2013). Both organizations then cited each other as sources for their work: in line with academic traditions of referencing, this was certainly intended to give their analyses more credibility (Albright, Brannan, & Walrond, 2011; ISIS, 2013; Mcdonald, O'Murchu, Doherty, & Chien, 2013). The United States Congressional Research Service (CRS), an organization that seeks to provide "timely, objective, authoritative and confidential" (Congressional Research Service website, 2014) research to members of the U.S. Congress, also drew on Symantec's analysis as a primary source (Kerr, Rollins, & Theohary, 2010). Then in 2011, in a research report "prepared for the Office of the Secretary of Defense," RAND drew upon Symantec's reports to draw out the technical features of a report they entitled the *Cyberworm that knows no boundaries* (Porche, Sollinger, & McKay, 2011, p. ii). This is a cursory sample of all the think tank and policy advice that drew upon Symantec's reports, but it is indicative of the extent to which the company's analyses were utilized in reports intended to shape the knowledge of policy and decision makers. However, as the later analysis will draw out, this reporting was not simply "objective" technical knowledge even if it was taken as such.

An immediate objection raised here would be to argue that the widespread citation of Symantec's reports merely represents a pragmatic division of labor. However, the point is not to refute the accuracy or the content of Symantec's work, but to challenge the ways that this knowledge gets "translated" into policy contexts and assembled into cybersecurity knowledge. Symantec also published and still maintain the website page for *W.32 Stuxnet* on their "Security Center" site (Shearer, 2019). This page contains the outline of the Infection, Functionality, Removal and "Technical Details," but none of the speculation and broader geopolitical context of the malware incident.

Yet, it was Symantec's blogs and whitepaper reports that were by far the most common source used by the subsequent coverage, not their "Technical Details" page. Symantec, like many vendors in the computer security industry, refer to their reports as "whitepapers," but given their format they are often taken as (neutral) technical reports of "the facts." As a case in point, a publication produced under the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) cited Symantec's analysis, amongst other vendors, in a report entitled *Stuxnet Facts Report: A Technical and Strategic Analysis* (De Falco, 2012). Meanwhile, the European Union Agency for Cybersecurity (ENISA) in its 2018 *Threat Landscape Report* similarly cited Symantec's analysis of Stuxnet, not their "Technical Analysis" webpage, and cited it along with a number of other vendors under the category of "Authoritative References" (ENISA, 2018, p. 29, 32). Symantec's reports nowhere use the word "cyber" or "cybersecurity," and yet their reports formed an integral part of the subsequent "cybersecurity" policy literature and think tank coverage. Further, while so much of the media coverage and subsequent policy-oriented interpretation of Stuxnet drew on the reports and blogs, this was instead of the still detailed but less narrative "Technical Details" posting on Symantec's website.

The formatting of their whitepapers is such that it gives the appearance of (objective) technical reporting. In both the *Stuxnet Dossier* and the *Stuxnet 0.5* reports, they include the detailed breakdown of different components and modules in the malware samples, and include graphs, diagrams, tables and code samples, presentation details that immediately connote a scientistic approach synonymous with other technical publications. Although Symantec appear to be careful in their use of terminology (describing the report as a dossier, and never referring to it as "technical analysis" per se), the presentation style of their "whitepaper" invokes a cultural vocabulary of "objective" and "scientific" knowledge. They do not discuss their methods or methodologies for analyzing the malware, and nor do they include any explicit claim of objective or technical expertise. However, as the selective range of publications highlighted above indicates, this has not precluded their reports from getting taken as a-political matters of fact. It is not that they were used and cited that needs to be given more consideration, but that *they were taken as a-political technical knowledge*. While Symantec and other commercial vendors may not intend for their work to be taken as objective, as it travels through different contexts and gets re-used and cited then its "authority" gets translated and concretized.

However, as this paper will demonstrate shortly, turning malware into an intelligible event is neither neutral nor a-political. Not only did Symantec's analysis thus get translated into discourses of "cybersecurity" as a matter of international political concern, the analysis later in this paper shows how they also themselves assembled a range of actors and materials to makes the malware meaningful as an event. Cybersecurity appears at a large number of locations and settings, each with its own set of practices and habits. Though only a tiny fraction of the overall landscape of multifarious processes and contexts that make up "cybersecurity" practices, reports such as Symantec's represent pivotal moments for understanding the processes in the "making" of cybersecurity. But as the next section will draw out, it is not just that the phenomena of cyberspace and cybersecurity are technically complex and difficult to grasp, but that they are also complex because they are made up of elements that necessarily exceed our capacity to know them. Here, the concept of "intangible artifacts" offers some useful insights for recognizing the political nature of such technical knowledge practices.

Materializing malware (or, materials and methods)

Stuxnet is a salient example of a class of politically contested artifacts that was embroiled in and contributed to geopolitical controversies. Here, the role of "intangible artifacts" can be a useful heuristic for the apparent challenges posed by security worlds (Rankin, 2014). Intangible artifacts are a class of objects that are "selectively visible, semi-permanent, and always flirting strategically with conventional forms of physicality," like radio waves, gamma rays, gas particles and toxic spills and other forms of politically contested but affective entities (Rankin, 2014, p. 625). At the smallest unit of analysis, Stuxnet is described as an example of computer code. Code is a series of instructions that transduce input and consequently performs work by interfacing the virtual (the world as 0s and 1s as on/off signals) with the material (Kitchin & Dodge, 2011). It lacks materiality in itself–code exists in the same way that speech or music exist, in that they have effects and can be represented and recorded to a media in textual form (Kitchin & Dodge, 2011, p. 24). The interesting thing about malware code is that it's productiveness, its ability to act, only emerges as it travels across materials, and interacts with the things its written on.

I suggest that malware is another example of this class of politically contested and contestable intangible objects. When "objects" in security studies may lack an obvious and immediately present materiality–for example only known at the level of rumor, or not fully disclosed (Walters, 2014)—then a new way of analyzing these objects is helpful. The first materialist element of this paper therefore follows on from Law and Singleton (2005), who argue that an examination of the ontological constitution of objects can "sensitize us to the way in which subjects and things can become active participants in political disputes" (Walters, 2014, p. 104).

Though the Stuxnet code lacks a physical materiality or corporeality except for the material it is "written" on or temporarily "trapped" in, by tracing the alliances made amongst and between the actors in these reports, analysts can interrogate the ways in which epistemic practices are embroiled in the making and defining of international cybersecurity practices. We should therefore ask how these intangible artifacts have been made "visible, persistent, and obdurate—through language, law, or their entanglements with more conventional objects" (Rankin, 2014, p. 664). Like other imperceptible hazards, apprehending the object and any risks that it poses requires its articulation and translation as such (Kuchinskaya, 2014). Such an analysis can therefore show where materiality is *making a difference* (Austin, 2017). Symantec's efforts are demonstrative of these kinds of productive efforts.

Intangible or opaque objects may be "made thingy" at different times and in different socio-historical contexts (Rankin, 2014), but these artifacts are not passive canvasses for representation. Dunn Cavelty (2018) has made a persuasive case for the need for an approach that can understand why some technologies elicit widespread reaction or political debate, whilst others stay in the background, uncontested or invisible. This means asking what kinds of incidents and materials become visible, and how: Symantec's reportage is a useful window into these practices, allowing us to trace how "technical" knowledge gets translated into official reports, legislation and political or partisan controversy. As the discussion so far has already touched upon, we have begun to trace how practitioners, international oriented actors, elected officials and military leaders amongst others hail or include or exclude certain technologies or artifacts in by drawing on specific readings of these incidents. Despite the opacity of these commercial practices and the technologies involved, and the difficulties posed by restricted access, by asking these kinds of questions an analysis can capture the dynamics that are helping to constitute cybersecurity in specific relational ways.

This article does not mean to dispute the technical abilities or capacities of Symantec's analysis. Instead, it is more concerned with demonstrating the political and strategic choices that were made through the company's coverage of the incident. The approach outlined in this paper thus enables us to interrogate the ways in which the very material existence of a thing itself can become a political matter.

The second materialist element to this article's method draws on Latour's (2005, 2007) and Walters's (2014) discussion of "public assemblies." Latour characterizes politics as being typified by realist epistemologies that presume in the presentation and assertion of indisputable facts–his counter to this is the concept of dingpolitik, or politics oriented around "matters of concern" and controversies (Latour, 2005, 2007). Walters builds on Latour's discussion, suggesting that such controversies are cases that cannot be resolved in the realist sense, because of the impossibility of calling on "a world of indisputable facts that exists outside any scheme of representation" (Walters, 2014, p. 104). Instead, such matters of concern are brought into public assemblies, which operate as sites of representation and knowledge production. As the discussion will show later, this article will showcase the analytical utility of approaching Symantec's analyses of Stuxnet as an example of a "public assembly" in this regard.

Analyzing commercial incident reports like Symantec's (or other companies such as Kaspersky and ESET's as the paper will shortly discuss) is helpful not because it allows us to draw general relationships between malware and international cybersecurity politics, but because it shows just how much the alliances forged in these reports are needed in order to turn "malware" into intelligible incidents or objects. Reports such as Symantec's are pivotal moments in the materialization of such traces, and it is these alliances and materials that serve to lend weight to both Stuxnet as code and Stuxnet as an assembly being mobilized by Symantec. As the analysis in the next section will illustrate, studying public assemblies (such as Symantec's analyses of Stuxnet) are thus a useful way into understanding some of the ways that intangible artifacts can evolve into of political matters of concern. It will also draw out a means of recognizing how materials are temporarily fixed or mobilized in these arrays. Public reports are knowledge-making practices, and how these assemblies define and mobilize objects are an important part of how cyberspace operations materialize in the public sphere.

The following analysis will predominantly draw upon three reports by Symantec: W32.Stuxnet (Falliere et al., 2011), Stuxnet 0.5: The Missing Link (Mcdonald et al., 2013) and will also discuss extracts from a series of posts on their Security Response blog dated between the 16th July 2010 until the date of the publication of the second Stuxnet 0.5 report in February 2013. This analysis will define the network being drawn into a public assembly by Symantec in their efforts to generate knowledge about Stuxnet.

Turning Stuxnet into an assembly and object

Symantec's report is full of dynamic and multifarious objects and actors: the computer program code, the operators of the targeted equipment, the creators of the code, the Programmable Logic Controllers (PLCs) and centrifuges, the uranium hexafluoride for enrichment and important organizations on the international stage as well as Symantec themselves. What Symantec strived to do was to bring all of these elements into an assembly by weaving a narrative of the Stuxnet "attack" that served to reinforce the importance of the incident for matters of international security

The object

The first aspect of their assembly focused around the "object" of the code itself. Throughout the reportage generated by Symantec, a piece of computer coding is demarcated and then described as "threat" and "malicious" Around these "malicious binaries" (Falliere et al., 2011, p. 3) Symantec draws in an assembly, turning this assembly into an object of knowledge (Stuxnet) as well as the piece of code that lies at the heart of the assembly. In their main report on Stuxnet, the researchers describe an "Attack Scenario," a narrative which helps to materialize the effects of the intangible code into its real world effects, even while admitting that it is "*speculation* [emphasis added] driven by the technical features of Stuxnet" (Falliere et al., 2011, p. 3). In this opening section, the affordances or technical capabilities of the code are what set it apart and concretizes the malware's effects: "Each feature of Stuxnet was implemented for a specific reason and for the final goal of potentially sabotaging the [Industrial Control Systems]" (Falliere et al., 2011, p. 3).

Symantec's analysis of Stuxnet discusses in detail the technical characteristics of the code that allowed it to proliferate across the computer networks in Iran and elsewhere, doing so in a way that turned it into an intelligible artifact. The code itself used a hitherto unparalleled range of characteristics to hide itself from operators of the targeted equipment. The list of Stuxnet's features are numerous, including the ability to circumvent antivirus programs, use stolen digital security certificates to fool systems into thinking the malware components are legitimate operations, an ability to search out very specific configurations of industrial equipment and then hide its presence from equipment operators by interrupting the security feedback information of that equipment by displaying data it had pre-recorded (Falliere et al., 2011). Symantec use a graphic to neatly distill the workflow or decision tree that the code goes through before it installs itself onto the system (Falliere et al., 2011, pp. 16–18). These kinds of diagrams and tables help to make Stuxnet an intelligible artifact.

For Symantec to be able to ascribe any intent to these modules and features though, they had to describe the technical affordances in detail: these capabilities do not speak for themselves. Furthermore, understanding their intent relies on witnessing their performance: "[T]he 'goodness' or 'badness' of software cannot be determined before said performance *and* its interpretation because it always incorporates a range of possible becomings in its code" (Balzacq & Dunn Cavelty, 2016, p. 7). In the case of Symantec's assembly, they had to establish the links between the fragments of decompiled code and the ways that it would execute in the targeted systems. This is like trying to recreate all the unfolding movements of a dance from a series of polaroid snapshots of static dancers. The way that programs perform cannot always be predicted or simply "read" from the decompiled code: Their performance or execution are immanent within the complex interleaving of code, firmware and hardware that makes up global networked ICTs (Joque, 2018). As a result, Symantec had to run some in virtual sandboxes and set up a simulated Step 7 Programmable Logic Controller (PLC) environment to observe it in action (Falliere, 2010; Zetter, 2014, p. 227). The malware would not speak for itself in its static form to reveal its target destination and intent. It required translation.

Symantec make several judgements in the way they draw their report together, beyond purely technical descriptions of the way the malware behaves. This "attack vectors" section of the report is a concise technical description of one element of the infection process, but goes one step further, drawing other actors and a wider political context into their assembly. This is not something they do in their "Technical Analysis" webpage (Shearer, 2019), suggesting that it was not simply a matter that they lacked the extra information for their webpage as the online resource is still maintained and updateable. Symantec describe one of the parameters that this infection process looks for. When a system has already been infected by the malware before, it leaves a marker in the registry of the system, a string of numbers which the malware looks for before infecting a system. If it finds that string in the registry, the process stops, and it proceeds no further. However, Symantec suggest that the number string–"19790509"–is a date, and one with political significance. In their report, they suggest that this

> date could be an arbitrary date, a birth date, or some other significant date. While on May 9, 1979 a variety of historical events occurred, according to Wikipedia "Habib Elghanian was executed by a firing squad in Tehran sending shock waves through the closely knit Iranian Jewish community. He was the first Jew and one of the first civilians to be executed by the new Islamic government. This prompted the mass exodus of the once 100,000 member strong Jewish community of Iran which continues to this day." (Falliere et al., 2011, p. 18)

This string of numbers was subject to a good deal of controversy amongst other security researchers and was declared "circumstantial evidence" at best (Cluley, 2010). While Symantec "cautions readers on drawing any attribution conclusions," they still decided to include this information in an otherwise code-based analysis section. ESET's report on Stuxnet also conducted a similar flow-analysis of Stuxnet's infection (Matrosov, Rodionov, Harley, & Malcho, 2010), but unlike Symantec, declined to draw wider associations into their report.

Symantec's analysis makes judgements in the links it forges in its assembly again in its discussion of a line of code in one of the malware's drivers. One of the file pathways in the driver is listed as:

```
b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb
```

Again, Symantec acknowledge that this is conjecture drawing on Wikipedia, but include the following in their report anyway:

> The string could have no significant meaning; however, a variety of interpretations have been discussed. Myrtus could be "MyRTUs". RTU stands for

> remote terminal unit and are similar to a PLC and, in some environments, used as a synonym for PLCs. In addition, according to Wikipedia, "Esther was originally named Hadassah. Hadassah means 'myrtle' in Hebrew." Esther learned of a plot to assassinate the king and "told the king of Haman's plan to massacre all Jews in the Persian Empire … The Jews went on to kill only their would-be executioners." (Falliere et al., 2011, p. 24)

Originally, Symantec had published the finding of this pathway on their blog in 2010, and it led to a good deal of speculation. In late 2010, F-Secure, a Finnish antivirus company, suggested that the RTU portion of myrtus could actually be an abbreviation for Remote Terminal Units, and indeed the Siemens PLCs described within the Stuxnet coding were a type of RTU (Bumgarner, 2013). Meanwhile, ESET's discussion of the file pathway simply stated that it was "interesting," and did not speculate any further (Matrosov et al., 2010, p. 13). Though Symantec were careful not to draw any conclusions from the data by pointing out that the file pathway may be alluding to remote terminal units, their reports are peppered with these additional alliances and links. These are more than just technical descriptions. By drawing these actors and events into their assembly, Symantec's researchers are translating the code into intelligible events while at the same time placing themselves into a wider political milieu.

The target of the code

Symantec explicitly draw the target of the code into the assembly. Because of the very specific and narrow parameters of the machinery and computers being sought within the malware's components, the Symantec report surmised that the designers of Stuxnet would have required a great deal of information in the form of schematics and design documents. The Symantec analysis describes the certain attributes that were assigned to the operators and users of the targeted systems by the designers. For example, it was known by the designers that the targeted systems were not connected to the internet and so the code was designed to be able to spread via removable drives (Broad, Markoff, & Sanger, 2011; Falliere et al., 2011; Mcdonald et al., 2013).

While the target of the code was widely interpreted to be a specific piece of equipment, Programmable Logic Controllers (PLCs), made by Siemens, in all three reports Symantec go further still by drawing nuclear facilities and PLCs located in Iran into their assembly.

> We could see in the code that it was looking for eight or ten arrays of 168 frequency converters each. You can read the International Atomic Energy Association's documentation online about how to inspect a uranium enrichment facility, and in that documentation they specify exactly what you would see in the uranium facility — how many frequency converters there will be, how many centrifuges there would be. They would be arranged in eight arrays

> and that there would be 168 centrifuges in each array. That's exactly what we were seeing in the code. (O'Murchu as cited in Fruhlinger, 2017)

The researchers thus had to translate what they "were seeing in the code" into intelligible events. But Symantec's researchers also realized that this had significant implications. As O'Murchu went on to describe it, "It was very exciting that we'd made this breakthrough. But then we realized what we had got ourselves into — probably an international espionage operation — and that was quite scary" (O'Murchu as cited in Fruhlinger, 2017). They did not draw these alliances into their detailed "Technical Description" webpage (Shearer, 2019), and yet *these* reports were the most widely cited in subsequent analyses of Stuxnet.

Despite their realization of their role in an "international espionage operation," they still drew the controversy of Iran's nuclear enrichment program into their assembly. In their 2013 report about Stuxnet 0.5 they specifically refer to the centrifuges involved in Iran's nuclear enrichment program at Natanz:

> Stuxnet 0.5 contains an alternative attack strategy, closing valves within the uranium enrichment facility at Natanz, Iran, which would have caused serious damage to the centrifuges and uranium enrichment system as a whole. (Mcdonald et al., 2013, p. 1)

This deployment of the materiality of the PLCs and centrifuges in the assembly makes the political matter of concern surrounding Iran's nuclear program a significant character in their analysis. At the crux of this "matter of concern" has been the uncertainty of Iran's objectives for their nuclear program. Despite the high frequency of IAEA site inspections and the statements issued by Iran about its peaceful intentions, the UN Security Council (UNSC) has been "seriously concerned that the International Atomic Energy Agency (IAEA) was still unable to provide assurances about Iran's undeclared nuclear material and activities" (UNSC, 2006). The centrifuges and PLCs are at the heart of the enrichment facilities in Iran, which have been subject to inspections and reports by the IAEA and the sanctions of the UNSC, as well as unilateral sanctions by members of the UNSC. All of these were drawn into Symantec's assembly.

Symantec's analysis of Stuxnet deploys the materiality of the centrifuges and PLCs as evidence–they act as spokespersons for these materials, describing their characteristics and operating parameters. Again, a comparison with ESET's coverage is insightful: they do not mention "nuclear enrichment," "Natanz," or "centrifuges" (Matrosov et al., 2010). Meanwhile, F-Secure mention the possibility of the Iranian enrichment program but suggest that it is one of many possible applications for the PLCs (F-Secure, 2010). The point here is not to contest Symantec's analysis, but to underscore the *judgments and decisions* that they made in the process of translating these traces into their assembly.

The presentation by Symantec of these centrifuges and Iran's enrichment facilities into their assembly thus intertwined their analysis with the materiality of Iran's nuclear program, lending durability to the assembly (Law, 1992). This also serves to relate to the debates about the material characteristics of things like the uranium particles being enriched, as the centrifuges are being convinced by the malware to interact with the uranium particles in a different way. After all, the uranium particles have to be "convinced" to separate in the manner that the designers of the centrifuges want (Scott Smith, 2013, p. 21). This in turn would work to imbricate the company into wider geopolitical "matters of concern," lending a weight to their analysis. This can also be understood as part of an effort to demarcate their legitimacy as authoritative sources of knowledge.

Making alliances with institutions and geopolitics

One of the recurring alliances that Symantec draw into their assembly is that of the creators of the Stuxnet code. No state actors had officially claimed responsibility for instigating the Stuxnet code and as Symantec acknowledged themselves, they "don't know who is behind the attack, and historically discovering this is very rare" (Fitzgerald, 2010). In the published reports, Symantec mostly refer to these parties as "attackers" as well as "hackers" and "bad guys," likening them to antagonists in a combative arena: Symantec's introduction to Stuxnet reinforces this narrative when they state that the "worm became known as the first computer software threat that was used as a cyberweapon" (Mcdonald et al., 2013, p. 1).

Stuxnet's complexity and modular design led researchers and the press to attribute the operation to government agencies, or possibly to some collaboration of agencies. However, the technical analysis of Stuxnet suggests some wider implications beyond the difficulties of ascribing "intent" and attribution to code. One of these technical characteristics that Symantec's researchers highlight are the functionalities intended to bypass specific brands of security products. Here, they describe the list of security products (antivirus software, firewalls and scanners) that the malware searches for to help it ascertain an installation process that will be most likely to avoid detection (Falliere et al., 2011, p. 13). Despite the effort that the programmers of Stuxnet went to circumvent detection softwares, Stuxnet surfaced as a threat because of a small Belarussian security company's VirusAdBloka software picking up unusual behavior by one of its customer's computers (Zetter, 2014, pp. 7–9). Although Stuxnet was programed to propagate across local area networks and removable drives rather than the internet, it still came to the attention of an international InfoSec community who subsequently reverse engineered and publicized its existence.

Symantec's investigation of this incident would not have been possible had the malware been able to fully account for the unexpected interactions with the enormously complex operating ecosystem, or the "vicissitudes of execution" (Chun, 2008) that might lead to its discovery. While the programmers had foreseen some of the most common obstacles posed to the operation by the complex interweavings of software, hardware and users, in the end it was its interaction with an obscure node of the network that brought it to the attention of security researchers.

As well as materializing the code in specific arrangements or networks, Symantec's reports have helped to concretize their legitimacy as experts, situating their role in an escalatory dynamic between this new class of threats and their roles as commercial researchers. The reference to attackers and "cyber weapons" can be understood as part of and contributing to a wider trajectory seen in policy discourse. This is exemplified by Symantec when they argued that "[t]he real-world implications of Stuxnet are beyond any threat we have seen in the past" (Falliere et al., 2011, p. 55). In their analyses, Symantec also draw the state-sponsorship of cyber security policy into the assembly, highlighting the alliances they have forged with state actors and organizations such as United States Computer Emergency Readiness Team (US-CERT) (Falliere et al., 2011, p. 5). One of the Symantec researchers who undertook the reverse engineering of the code said in 2017 that it was the most complex code the team had reviewed and was "in a completely different league from anything we'd ever seen before" (O'Murchu as cited in Fruhlinger, 2017). For the researchers, this meant that they have had to develop better toolsets to respond to these evolving threats and malware:

> What we hope is that we've advanced to make it more difficult for them to do things and not be noticed. … I would hope we'll be able to find them faster and see traces, but you never really know. We could be missing a bunch of stuff now. (O'Murchu as cited in Jackson Higgins, 2019)

A principal security researcher at Kaspersky was more forthright in their assessment: "We see this battle or arms race emerging and now it involves some kind of confrontation between the security industry and nation-state sponsored spies" (Vitaly Kamluk as cited in Goodin, 2015). For Symantec, Stuxnet represented a precedent where countries around the world realized the possibilities that Stuxnet represented, that what had been hypothetical was now possible and that these countries "should get into this too" (Chien as cited in Miller, 2016). As a result, Symantec would be able to position itself as uniquely qualified to study and publicize such malware incidents:

> Basically, every country you can imagine has decided that they want to start some sort of cyber-offensive campaign, and so in that sense, the way to handle those threats and understand them and dig into them, the complexity of them, is much, much greater now. (Chien as cited in Miller, 2016)

By using its reports to forge links and alliances, Symantec thus defined a particular identity for itself as knowledgeable experts and as a reliable resource in the field of computer security, positioning themselves as crucial barriers to "attackers."

This is not about the delegation of previously state security responsibilities, but about the role that commercial actors are forging (and having to forge) for themselves in response to an evolving landscape. Their role as experts in this field, and the operations and incidents that they are observing, are to some extent co-producing each other. As an intangible artifact, it is difficult to know when malicious code is present, other than when systems or targets start behaving in unexpected ways. It is possible for malware to be dormant too. As a result, a vast number of technological systems, sensors, programs and a whole industry have sprung up in order to trace their residues and effects for customers. Although the malware included AV-avoidance, those same companies ended up deconstructing the malware and making their own reports. These mechanisms and programs have their own economy: they are intellectual property, unaccountable. It also requires a significant technical knowledge to trace. Nor do commercial antivirus or "Threat Intelligence" reports include explicit discussions of methodologies. Although the reports of companies such as these afford us an insight into how of intangible artifacts like malware get made durable or concrete through representation, we must also be cognizant of the potential biases and judgements in such reports.

Symantec's analyses are filled with technical terminology and specific language related to computer programing. In itself this is not surprising as they are self-proclaimed detailed analyses from an organization dedicated to a specialized epistemic field. However, these reports are not purely objective, but represent a series of judgements and decisions about the alliances they forge through their reports. Symantec's analyses promulgates both this form of knowledge and an impression of their expertise which I suggest is significant because of the organizations and types of conceptual, material and textual alliances their analysis has mobilized. The enrollments and acts of translation that Symantec have presented in their analysis have taken part in a broader trajectory, in which their knowledge has been integrated into wider statist concerns with "cybersecurity," as demonstrated in the breadth of their subsequent citations in policy-oriented reports on Stuxnet.

Theirs was a strategic mobilization and other courses of action were open to them: In other instances, computer security companies acknowledge that "[p]erforming attribution in a serious, scientific manner is a hard problem that is out of scope of [our company's] mission" (ESET, 2016, p. 11). Similarly, Facebook's white paper on information operations also carefully pointed out that "Facebook is not in a position to make definitive attribution to the actors sponsoring this activity" (Weedon, Nuland, & Stamos, 2017, p. 11), instead pointing to officially sanctioned reports from the US Office of the Director of National Intelligence. In Symantec's case, the alliances they make throughout their assembly are thus productive of both Stuxnet as an object as well as of a wider field of cybersecurity.

Conclusion: Assembling cybersecurity

The analysis of Symantec's reports, and its comparison with other companies' work, shows that such efforts at turning malware into an intelligible event are neither neutral nor a-political. As well as getting translated into discourses of "cybersecurity" as a matter of international political concern, Symantec's analysis mobilized an assembly of materials and spokespersons, which turned Stuxnet into more than just an object (the code) in the physical and relational sense. Symantec instrumentally mobilized particular alliances in their assembly, to turn the code into an intelligible object and event. For example, by bringing the uranium hexafluoride particles and the centrifuges at Natanz explicitly to the assembly, they also served to bring to presence the IAEA, the UNSC and the political controversy that surrounds Iran's nuclear enrichment program. Theirs is an example of performative processes of sense-making.

This approach has sought to demonstrate the politically situated nature of how cybersecurity expertise emerges, showing that in Symantec's case, theirs was not a-political or neutral technical work: They made profoundly political choices in their analyses. Given these strategic choices in how they present the evidence, it is likely that they were trying to "sell" their expertise, but we must be cognizant of these kinds of political economies and pay attention to how these reports get translated into wider policy framings and discourses. Their publications were a formative instance of these emerging dynamics. In future, future this materialist-minded approach could fruitfully be used to analyze other instances, such as "Threat Intelligence" firms and their involvement in attribution and foreign policy debates. Assemblies and reports such as Symantec's offer an insight into how these controversial matters and intangible artifacts can get concretized. It can also show us how these assemblies then get mobilized and translated into knowledge about and concerned with "cybersecurity."

Three important points arise, both analytically and reflexively. Firstly, this analysis has sought to demonstrate the importance of capturing all the actors and materials in an assembly like Symantec's without predeciding how to categorize all the elements in the assembly, whether into categorical distinctions such as "public-private" or between material-human intention and agency. It is not simply a matter of "private" firms performing "public" security functions or of thinking of them as private security actors in the sense that this Weberian categorical distinction would imply. Symantec's role is something more diffuse, or more "hybrid" than such a framing would allow for

(Leander, 2014). By paying attention to the materiality and affordances presented by such actors, without pre-judging (and potentially reifying these categories), the analysis has begun to trace all the things that made a *difference* in the outcome of an operation, controversy or incident. This can help us understand the context and the facilitating conditions for subsequent policies and discourse, as well as the kind of politics that stem from such arrangements.

Secondly, paying attention to materials, to intangible artifacts, though only ever partial, and showing where they resist or refused, shows us how secret operations are not just acts of occluding/hiding information, of segregating knowledge, but are intensely spatial and material. These are insights already artfully demonstrated in the literature on secrecy practices that bear examination in the light of cybersecurity knowledge practices (Anaïs & Walby, 2016; Birchall, 2014; Paglen, 2010). This approach casts a critical eye on the way that the traces are produced by technics and spokespersons. But as Latour and others have long emphasized, the production of scientific and technical "facts" require effort and are distinctly relational processes (Latour & Woolgar, 2013). These knowledge-making processes of commercial firms are not devoid of their economic and commercial incentives either: there is a political economy here, but also a symbiotic relationship between the designers of these pieces of malware and the researchers who research and mitigate against them. Not only are malware incidents seemingly growing in complexity and scope, they are also necessitating more and more complex technical knowledge to mitigate, thus empowering or enlisting the involvement of a whole range of actors that exceeds straight-forward categorization as either "public" or "private." Utilizing their labor is a pragmatic response – a division of labor, as they have the skills and the insight into customers systems the world over which state actors do not. But what are the repercussions? How can we conceptualize these dynamics, the political power that such companies may accrue through these reports? The materialist approach proposed here has sought to illuminate just these sorts of questions.

Thirdly, a reflexive and perhaps normative point then, is that this kind of analysis is also a tool to minimize reifying those binary distinctions such as "public" and "private" through our analysis without a consideration of the rationales for such conceptual boundaries. As McCarthy has insightfully argued, if we are to understand who and what cybersecurity is *for*, without reproducing existing liberal social formations, we can begin to "articulate the wider stakes of cybersecurity with greater clarity" (McCarthy, 2018, p. 6). It is towards this "deepening" of security frameworks that this article has sought to contribute.

This article has not engaged in criticism of the substance of such assemblies–it has not tried to argue that the specific analyses conducted by these companies are wrong, or that the involvement of commercial firms more generally is suspect. Instead, it has pointed to the differences in versions of the malware presented by the companies, and suggest that these analyses will lead to different conceptions of what to do, or what makes good policy, or what political and technical responses to malware can or should look like in the future. If cybersecurity is a complex arrangement of practices and actors still "in the making," and if decisions about "right" and "wrong" cybersecurity policies and roles are at stake, then these decisions are only possible if we have a standard to work from. In other words, we must consider who and what cybersecurity is for if we are able to make such judgements (McCarthy, 2018; Mol, 2002). Who gets responsibility for cybersecurity? What role can and should commercial actors play in threat intelligence provision? Is there a political economy that may shape the development of these analyses? These questions are still open to debate nearly a decade after Symantec's analyses, but value judgements about who and what cybersecurity are for are implicated when cybersecurity policies take such analyses as objective reports. In other words, the empirical argument of this article is largely about the need to be more reflexive about the use and assumptions of the long-held conceptual distinctions between "public" and "private" to show how these rationales may not neatly map into cybersecurity.

Taking the technical work of commercial firms as unquestioningly a-political and neutral means that it may come to shape the available policy options in unforeseen ways. Rather than asking is this policy *effective*, we should also be asking what *effects* the policy may be having, and if they are for the good. The role of commercial firms in making "good" cybersecurity knowledge is thus an important area for future investigations.

Notes

1. More recently, companies also refer to themselves as "Threat Intelligence" firms, while those working in the industry often prefer to call themselves "InfoSec" (information security) researchers, rather than "cyber" or "cybersecurity" which predominates in statist discourses (Shires & Smeets, 2017; Slowik, 2019).
2. But see Banks (2015).

Acknowledgements

Portions of this article are drawn from an un-published MSc dissertation submitted to the University of Bristol in 2014. The author would like to thank Dr. Myriam Dunn Cavelty and all the participants at the ETH Zurich Cybersecurity Conference in 2018 for their helpful suggestions and stimulating discussions. She would also like to thank Pieter Lagerwaard, Tasniem Anwar, Esmé Bosma and all the participants at the 2019 EISA Sofia Early Career Workshop "Writing Methods: Encountering Secrecy and 'Mess' in Security Research" for their vital input and camaraderie. Finally, my thanks to Lilly Muller for her invaluable support in seeing this paper through to its current form. Any errors remain my own.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by the Economic and Social Research Council (Grant number ES/P000630/1).

Notes on contributor

Clare Stevens is based at the South West Doctoral Training Partnership (SWDTP) and the University of Bristol. She is also an Assistant Teaching in Politics and Sociology and is completing an interdisciplinary Ph.D. thesis on the strategic use and misuse of cyberspace by state and non-state actors. Using the idea of "boundary work" as an organizing heuristic for her analysis, she is investigating the ways that U.S. state actors talk about cybersecurity and cyber operations are shaping or challenging understandings of "old" strategic concepts or social categories and boundaries.

ORCID

Clare Stevens http://orcid.org/0000-0002-5685-7930

Reference list

Albright, B., Brannan, P., & Walrond, C. (2010). *Institute for science and international security Did Stuxnet Take Out 1, 000 Centrifuges at the Natanz enrichment plant?* Retrieved from http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Albright, D., Brannan, P., & Walrond, C. (2011). *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*. Retrieved from http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/

Albright, D., & Stricker, A. (2010). ISIS Reports Stuxnet worm targets automated systems for frequency converters: Are Iranian centrifuges the target? Retrieved from http://isis-online.org/isis-reports/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-is-irans-ce/8

Anaïs, S., & Walby, K. (2016). Secrecy, publicity, and the bomb: Nuclear publics and objects of the Nevada Test site, 1951–1992. *Cultural Studies*, *30*, 949–968. doi:10.1080/09502386.2015.1113553

Aradau, C. (2010). Security that matters: Critical Infrastructure and objects of Protection. *Security Dialogue*, *41*, 491–514. doi:10.1177/0967010610382687

Austin, J. L. (2017). We have never been civilized: Torture and the materiality of world political binaries. *European Journal of International Security*, *23*, 49–73. doi:10.1177/1354066115616466

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*, 176–198. doi:10.1017/eis.2016.8

Banks, J. (2015). The Heartbleed bug: Insecurity repackaged, rebranded and resold. *Crime, Media, Culture*, *11*, 259–279. doi:10.1177/1741659015592792

Best, J., & Walters, W. (2013). Translating the sociology of translation. *International Political Sociology*, *7*, 345–349. doi:10.1111/ips.12026_5

Birchall, C. (2014). Aesthetics of the secret. *New Formations*, *83*, 25–46. doi:10.3898/NeWf.83.03.2014

Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the European Union. *Crime, Law and Social Change*, *67*, 219–247. doi:10.1007/978-3-319-63010-6_10

Broad, W., Markoff, J., & Sanger, D. (2011). Israeli test on worm called crucial in Iran nuclear delay. *New York Times*. Retrieved from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Bumgarner, J. (2013). A virus of biblical distortions. Retrieved from https://www.darkreading.com/attacks-breaches/a-virus-of-biblical-distortions/d/d-id/1141007

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*, 43–62. doi:10.1111/1468-2346.12504

Christensen, K. K., & Petersen, K. L. (2017). Public-private partnerships on cyber security: A practice of loyalty. *International Affairs*, *93*, 1435–1452. doi:10.1093/ia/iix189

Chronicle. (2019). Who is Gossipgirl? Retrieved from https://medium.com/chronicle-blog/who-is-gossipgirl-3b4170f846c0.

Chun, W. H. K. (2008). On "sourcery," or code as fetish. *Configurations*, *16*, 299–324. doi:10.1353/con.0.0064

Cluley, G. (2010). 19790509: The mysterious number inside the Stuxnet worm. Retrieved from https://nakedsecurity.sophos.com/2010/11/23/19790509-the-mysterious-number-inside-the-stuxnet-worm/

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, *6* (2), 13–21. doi:10.17645/pag.v6i2.1324

Congressional Research Service website. (2014). Mission (About Us). Retrieved from http://www.loc.gov/crsinfo/about/

De Falco, M. (2012). Stuxnet facts report: A technical and strategic analysis. *NATO Cooperative Cyber Defense Centre of Excellence*. Retrieved from: https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/

De Goede, M. (2018). The chain of security. *Review of International Studies*, *44*, 24–42.

Dunn Cavelty, M. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, *6*(2), 22–30. doi:10.17645/pag.v6i2.1385

Dunn-Cavelty, M., & Suter, M. (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187. doi:10.1016/j.ijcip.2009.08.006

Eichensehr, K. E. (2017). Public-private cybersecurity. *Texas Law Review*, *95*, 467–538. doi:10.3868/s050-004-015-0003-8

ENISA. (2018). *ENISA Threat LANDSCAPE REPORT 2018: 15 Top Cyberthreats and trends*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

ESET. (2016). *En Route with Sednit*. Retrieved from http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

F-Secure. (2010). Stuxnet Redux Q&A. Retrieved from https://www.f-secure.com/weblog/archives/00002066.html

Falliere, N. (2010). Exploring Stuxnet's PLC Infection Process. Retrieved from https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

Falliere, N., O'Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet dossier version 1.4 (February 2011)* (Vol. 4). Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. doi:10.1080/00396338.2011.555586

Fitzgerald, P. (2010). The hackers behind Stuxnet. Retrieved from http://www.symantec.com/connect/blogs/hackers-behind-stuxnet

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work? Retrieved from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Goodin, D. (2015). Stepson of Stuxnet stalked Kaspersky for months, tapped Iran nuke talks. Retrieved from https://arstechnica.com/information-technology/2015/06/stepson-of-stuxnet-stalked-kaspersky-for-months-tapped-iran-nuke-talks/

ISIS. (2013). *Basic attack strategy of Stuxnet 0.5*. Retrieved from http://isis-online.org/uploads/isis-reports/documents/Stuxnet_attack_strategy_26Feb2012.pdf

Jackson Higgins, K. (2019). New Twist in the Stuxnet Story. Retrieved from https://www.darkreading.com/threat-intelligence/new-twist-in-the-stuxnet-story/d/d-id/1334511

Joque, J. (2018). *Deconstruction machines: Writing in the age of cyberwar*. Minneapolis, MI: University of Minnesota Press.

Kearns, O. (2016). State secrecy, public assent, and representational practices of U.S. covert action. *Critical Studies on Security*, *4*, 276–290. doi:10.1080/21624887.2016.1246305

Kearns, O. (2017). Secrecy and absence in the residue of covert drone strikes. *Political Geography*, *57*, 13–23. doi:10.1016/j.polgeo.2016.11.005

Kerr, P. K., Rollins, J., & Theohary, C. (2010). *The Stuxnet computer worm: Harbinger of an emerging warfare capability (CRS report for congress No. R41524)*. Washington, DC: Congressional Research Service.

Kitchin, R., & Dodge, M. (2011). *Code/space: Software and everyday life*. Cambridge, MA: The MIT Press.

Kuchinskaya, O. (2014). *The politics of invisibility: Public knowledge about radiation health effects after Chernobyl*. Cambridge, MA: The MIT Press.

Latour. (2005). From realpolitik to dingpolitik or how to make things public. *Human Relations*, *69*(5), 4–31. doi:10.1177/0018726715600230

Latour, B. (2007). Turning around politics. A note on Gerard de Vries' paper. *Social Studies of Science*, *37*, 811–820. doi:10.1177/0306312707081222

Latour, B., & Woolgar, S. (2013). *Laboratory life: The construction of scientific facts*. Princeton, NJ: Princeton University Press.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems Practice*, *5*, 379–393. doi:10.1007/BF01059830

Law, J., & Singleton, V. (2005). Object lessons. *Organization*, *12*, 331–355.

Leander, A. (2014). Understanding US national intelligence: Analyzing practices to capture the chimera. In J. Best, & J. Gheciu (Eds.), *The return of the public in global governance* (pp. 197–221). Cambridge: Cambridge University Press.

Lundborg, T., & Vaughan-Williams, N. (2015). New materialisms, discourse analysis, and international relations: A radical intertextual approach. *Review of International Studies*, *41*, 3–25. doi:10.1017/S0260210514000163

Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). *Stuxnet under the microscope (Revision 1.1). ESET*. Retrieved from http://ece.wpi.edu/~dchasaki/papers/Stuxnet_Under_the_Microscope.pdf

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. doi:10.17645/pag.v6i2.1335

Mcdonald, G., O'Murchu, L., Doherty, S., & Chien, E. (2013). *Stuxnet 0.5: The Missing Link*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/stuxnet-missing-link-13-en.pdf

Miller, J. (2016, June). What We Learned About Cyber Warfare From the Heroes of Stuxnet. *New Yorker Magazine*. Retrieved from http://nymag.com/intelligencer/2016/06/what-we-learned-about-cyber-warfare-from-the-heroes-of-stuxnet.html

Mol, A. (2002). *The body multiple: Ontology in medical practice*. Durham, NC: Duke University Press.

Paglen, T. (2010). Goatsucker: Toward a spatial theory of state secrecy. *Environment and Planning D: Society and Space*, *28*, 759–771. doi:10.1068/d5308

Porche III, I. R., Sollinger, J. M., & McKay, S. (2011). *A cyberworm that knows no boundaries*. Santa Monica, CA: RAND.

Rankin, W. (2014). The geography of radionavigation and the politics of intangible artifacts. *Technology and Culture*, *55*, 622–674. doi:10.1353/tech.2014.0077

Schouten, P. (2014). Security as controversy: Reassembling security at Amsterdam Airport. *Security Dialogue*, *45*, 23–42. doi:10.1177/0967010613515014

Scott Smith, T. (2013). *The least provocative path: An ANT lens on development project formation and dissolution* (Actor-Network Theory for Development No. 3). Retrieved from http://www.cdi.manchester.ac.uk/resources/ant4d.

Shearer, J. (2019). W.32 Stuxnet Write-up. Retrieved from https://www.symantec.com/security-center/writeup/2010-071400-3123-99

Shires, J., & Smeets, M. (2017). *Contesting "cyber."* Retrieved from https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/contesting-cyber/

Slowik, J. (2019). Extracting community from the communitarian. Retrieved from https://pylos.co/2019/04/24/extracting-community-from-the-communitarian/.

Stevens, T. (2018). Editorial: Global cybersecurity: New directions in theory and methods. *Politics and Governance*, *6*(2), 1–4. doi:10.17645/pag.v6i2.1569

UNSC. (2006, July 31). Security council demands Iran suspend uranium enrichment by 31 August, or face possible, economic, diplomatic sanctions. *Security Council Press Release, SC*/8792. Retrieved from https://www.un.org/press/en/2006/sc8792.doc.htm

Van Veeren, E. (2014). Materializing US security: Guantanamo's object lessons and concrete messages. *International Political Sociology*, *8*, 20–42. doi:10.1111/ips.12038

Walters, W. (2014). Drone strikes, dingpolitik and beyond: Furthering the debate on materiality and security. *Security Dialogue*, *45*, 101–118. doi:10.1177/0967010613519162

White House. (2003). *The national strategy to secure cyberspace*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Weedon, J., Nuland, W., & Stamos, A. (2017). Information operations and Facebook. *Facebook*. doi:10.1016/B978-1-4377-2003-7.00058-3

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York, NY: Broadway Books.