Contemporary Security Policy

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

Cyber-noir: Cybersecurity and popular culture

James Shires

To cite this article: James Shires (2020) Cyber-noir: Cybersecurity and popular culture, Contemporary Security Policy, 41:1, 82-107, DOI: 10.1080/13523260.2019.1670006

To link to this article: https://doi.org/10.1080/13523260.2019.1670006

Published online: 22 Sep 2019.

CONTEMPORARY SECURITY POLICY
2020, VOL. 41, NO. 1, 82–107
https://doi.org/10.1080/13523260.2019.1670006

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Cyber-noir: Cybersecurity and popular culture

James Shires

Institute for Security and Global Affairs, University of Leiden, The Hague, The Netherlands

ABSTRACT

Cybersecurity experts foster a perception of cybersecurity as a gloomy underworld in which the good guys must resort to unconventional tactics to keep at bay a motley group of threats to the digital safety of unsuspecting individuals, businesses, and governments. This article takes this framing seriously, drawing on film studies scholarship that identifies certain aesthetic themes as associated with moral ambiguity in noir films. This article introduces the term "cyber-noir" to describe the incorporation of noir elements in cybersecurity expert discourses. It argues that the concept of cyber-noir helps explain the persistence of practices that blur legal, moral, and professional lines between legitimate and malicious activity in cyberspace. Consequently, changing cybersecurity requires not only institutional and technological measures, but also a re-constitution of cybersecurity identities themselves.

KEYWORDS Cybersecurity; popular culture; film; threat intelligence; noir; narrative

Dark Trace. Digital Shadows. Dark Cubed. Carbon Black. Dark Matter. Many emerging companies in the cybersecurity industry deliberately play on the popular perception of cybersecurity as a nether region, a gloomy underworld in which the good guys must resort to unconventional tactics to keep at bay a motley group of threats to the digital safety of unsuspecting individuals, businesses, and governments. These purveyors of what might be called "cyber-noir"–defined as the incorporation of noir aesthetics and themes into expert cybersecurity discourses–are often dismissed in International Relations (IR) as a mere sideshow, a footnote to more comfortable state-based dynamics. This article does the opposite. It takes the branding of the cybersecurity industry seriously, asking why these companies seek to portray liminality, transgression, and tantalizing opacity. Is it, as a (relatively) viral video of Michael Sulmeyer, former Director of Harvard Kennedy School's Cybersecurity Project, put it,

CONTACT James Shires j.shires@fgga.leidenuniv.nl Institute for Security and Global Affairs, University of Leiden, Turfmarkt 99, 2511 DP, The Hague, The Netherlands

This article has been republished with minor changes. These changes do not impact the academic content of the article.

just an effort to conjure up "cybersecurity sex appeal" (Sulmeyer, 2016)? Or is there something else going on–something more fundamental to cybersecurity itself, and more theoretically interesting?

This article puts forward the concept of cyber-noir to capture the interaction between two discourses: an expert discourse of cybersecurity and a wider noir discourse circulating primarily in popular culture artefacts such as films, books, and television series. It approaches this interaction from a post-structural perspective, understanding discourses not as collections of texts produced by already fixed actors, but as defining and constraining the identities of those actors, and through discursive overlaps and tensions generating meaning and providing conditions of possibility for action. Unlike other post-structuralist works in security studies, which often prioritize readings of popular culture artefacts as political texts, this article instead focuses on the appearance of popular culture elements in specific expert practices. It argues that the concept of cyber-noir helps explain the persistence of expert practices that blur legal, moral, and professional lines between legitimate and malicious activity in cyberspace.

The article is structured in four sections. The first section argues that distinct cybersecurities noted by securitization scholars share a common distinction between legitimate and malicious activity, and that cybersecurity experts work to maintain this distinction against technological, economic, and social factors that threaten to undermine it. The second section provides the theoretical basis for the concept of cyber-noir, drawing on film studies, critical security studies, and wider postmodern thought, including that of Baudrillard, to justify the article's focus on popular culture influences on cybersecurity such as noir, science fiction, and cyber-punk. The third and fourth sections analyze two aspects of cybersecurity expert discourses: visual styles and naming conventions. These sections trace noir influences on images and names circulating in these discourses, arguing that these influences create and sustain a morally ambiguous expert identity, which in turn perpetuates practices that blur the legitimate/malicious boundary. To paraphrase a neat description of film noir leads, cybersecurity experts see themselves as "seeming black and then seeming white, and being both all along" (Luhr, 2012, p. 32). Consequently, the deepest difficulty in maintaining the legitimate/malicious binary–and therefore constructing a stable foundation for cybersecurity itself–is not the range of technological, social, and economic pressures explicitly recognized by cybersecurity experts, but their implicit embrace of cyber-noir.

Legitimate and malicious activity in cyberspace

This section locates the article in existing cybersecurity theory in International Relations (IR) scholarship. It argues that a foundational problem in cybersecurity is the task of drawing a clear dividing line between legitimate and malicious activity in an environment swamped with data, where identical tools and tactics are used for different ends, and where social and economic structures compound technical similarities.

Hansen and Nissenbaum (2009) have argued influentially that cybersecurity, as an emerging discourse in international security, is the product of a technical computer security discourse plus securitization: the framing of international political issues as problems of security (Buzan, Waever, & Wilde, 1997). A large literature has critically examined the securitization of cyberspace (e.g., Barnard-Wills & Ashenden, 2012; Bendrath, 2001; Lee & Rid, 2014; Zajko, 2015), highlighting that cybersecurity threats are the contingent result of particular communications to a receptive audience. As Dunn Cavelty has shown, this securitization is not dependent on a single speech act, but has a complex genealogy (2008a, 2008b), and relies on less visible actors to shape threat perceptions (2013). The most exaggerated cybersecurity threats, termed "cyber-doom" by Lawson (2013), are apocalyptic scenarios of state collapse, widespread injury, and death. Although the state unsurprisingly dominates IR literature as the main "referent object" for cyber-securitizations, other referent objects do exist. Liberal personhood, digital systems, and profit-oriented organizations have all been proposed as alternatives (Deibert, 2018; Flyverbom, Deibert, & Matten, 2017; Shires, 2019). Overall, this literature demonstrates that cybersecurity consists of multiple overlapping, sometimes contradictory, and sometimes failed security discourses.

A common thread running through these diverse cybersecurity discourses is a binary distinction between the terms "legitimate" and "malicious," in descriptions of specific digital communications, wider patterns of activity, and attached to individuals, organizations, and states. This binary distinction stems from the original technical discourse of computer security, focused on the maintenance of formal definitions of confidentiality, availability, and integrity of communications channels against well-specified adversary capabilities. The distinction can be found throughout the different cyber-securitizations above, incorporating a range of referent objects. This "intentional ambiguity" has problematic consequences, as it represents both a point of contact and site of contest between different cybersecurity discourses (Shires, in press). Nonetheless, the existence of a focal point at which different securitizations converge enables the treatment of varied cybersecurity discourses together, as centered on a distinction between legitimate and malicious cyber activity. Moreover, one of the main tasks of cybersecurity experts is to continually re-draw this line: defining what is within and outside the sphere of legitimate activity, and thereby repeatedly re-affirming the distinction itself. Cybersecurity experts explicitly conduct this definitional work against three kinds of countervailing pressures.

First, they see the technological characteristics of cyberspace as an obstacle to the legitimate/malicious distinction. Because cyber-attacks exploit logical flaws in digital systems, intruders seek to mimic legitimate activity as closely as possible: in the oft-quoted words of Libicki (2010), "there is no forced entry in cyberspace." For example, while "legitimate" users enter a string of text in a website password field, "malicious" actors insert executable code that extracts information from the underlying database; but the executable code is still text, just with different characters. More generally, many computer viruses are downloaded from what appear to be "legitimate" emails or websites. These viruses locate themselves in standard system processes, obfuscating their "malicious" components and creatively manipulating "legitimate" routes to receive commands and exfiltrate data. Often, "malicious" actors simply repurpose "legitimate" tools and programs, like remote shells or data deletion software (Bronk & Tikk-Ringas, 2013). In addition, the sheer volume of information passing through digital networks means that cybersecurity defenses must make a trade-off between allowing "legitimate" communications while simultaneously preventing "malicious" ones; however, at such scales even a small margin of error means that the two are often confused. Finally, Gartzke and Lindsay (2015) highlight the prevalence of deception on both sides, because while attacks imitate benign communications to gain entry and avoid detection, defenders also exploit technical characteristics of cyberspace to set up realistic digital "honeypots," luring attackers into believing they are entering genuine systems.

Second, cybersecurity experts also view themselves as maintaining the legitimate/malicious distinction against contrary economic and institutional dynamics. Factors include: institutional structures placing offensive and defensive actors in the same organization, such as government intelligence agencies, and sometimes in the same room (Kaplan, 2017); a lack of regulatory and legal frameworks preventing private companies from "hacking back" against attackers to prevent further economic loss (Kello, 2019); and low-risk high-reward dynamics enticing individuals to sell vulnerabilities and exploits on black and grey markets (Fidler, 2015). Although these practices all blur the line between legitimate and malicious activity, the economic and social structures most frequently cited in this vein are penetration or "pen" testing and bug bounty programs, where either specific companies are paid to simulate a cyberattack on a system, or an open call is made to any cybersecurity researcher to do the same for financial reward depending on the scale of the vulnerability found (Ellis, Huang, Siegel, Moussouris, & Houghton, 2018). The prevalence of pen testing and bug bounties means that many "malicious" tools can be developed and acquired legally, with the justification that they are designed only for carefully limited uses.

A third obstacle locates difficulties in the constitution of the field itself, pointing to the contradictory ideas of security in cybersecurity discourses explored above. Cybersecurity experts identify two kinds of difficulties in maintaining the legitimate/malicious distinction in relation to different referent objects. The first concerns different referent objects of the same kind with competing self/other representations. For example, for the United States, its own offensive cyber activity is “legitimate” national security espionage while similar Chinese activity is nearly always “malicious” intellectual property theft (Paletta, 2015). More complicated contradictions emerge between different categories of referent object. Following wider debates in security studies between national and human security (Paris, 2001), these two cyber-securitizations lead to opposite definitions of legitimate and malicious activity. “Legitimate” state surveillance of cyber threats, in the former, becomes itself a “malicious” cyber threat to individuals in the latter, while “legitimate” freedom of expression from an individual perspective becomes a “malicious” cyber threat to state information control (Deibert, Palfrey, Rohozinski, & Zittrain, 2011; Shires, 2019).

These explicit obstacles to the distinction between legitimate and malicious cyber activity are well recognized in the cybersecurity literature, and I do not mean to diminish their importance in this article. Instead, I want to highlight another factor that is implicit but no less important. To preview the argument below, I suggest that the difficulty of distinguishing legitimate and malicious activity is also a result of popular cultural influences on expert cybersecurity discourses. These influences produce cybersecurity identities that are liminal and transgressive, moving fluidly between “legitimate” and “malicious” practices. To appreciate such popular cultural influences, we need to move from the constructivist basis of securitization theory towards post-structural theories of discursive constitution and interaction. As Guzzini (2000) has argued, the two theoretical approaches are not necessarily opposed, as long as the critical origins of securitization theory are emphasized (Barkin & Sjoberg, 2019). Without space to enter further into this debate here, I merely wish to note that some strands of securitization theory, such as the “Paris” school focusing on the security practices of “professional managers of unease” (Bigo, 2002, p. 74), have strong affinities with my focus on experts (Balzacq, 2010; Bigo, 2008; for further developments Van Rythoven, 2015). I use the term “discourses” as well as “practices” in this article, recognizing that this conceptual relationship is complex and practices are not “off-limits” to post-structural theorists (Adler & Pouliot, 2011; Hansen, 2006) The upshot is that this article does not analyze key moments of securitization, such as securitizing speech acts, their venue, or audience, instead focusing on more “everyday” popular cultural elements of expert discourses.

This argument is relevant to IR scholars outside cybersecurity, fitting into a broader literature on popular culture and international politics. It follows Weldes’ call to “go cultural” in the study of IR, with the rationale that “[political] representations are themselves made sensible in no small part precisely because they fit with, or articulate to, the constructions of the world and its workings into which diverse publics are hailed in their everyday lives” (1999, p. 133). These scholars use diverse theoretical approaches including securitization theory (Vuori, 2010; Williams, 2003), poststructuralism (Campbell, 2003; Derian, 2005), and sociological theories of risk (Amoore, 2007) to shed new light on familiar security subjects such as war, terrorism, border control, and nuclear proliferation. More recent work has taken this inspiration in a range of fascinating directions (Jones & Paris, 2018; Kiersey & Neumann, 2013; Musgrave, 2019; Neumann & Nexon, 2006; Young & Carpenter, 2018) For these scholars, popular culture artefacts are not merely ephemera of state-based dynamics but both an expression of and influence on policymakers' and citizens' identities, attitudes, and desires.

Many of the studies above prioritize readings of popular culture artefacts as political texts over reading politics in the categories of popular culture. Partly this is due to a choice of empirical data, as these scholars conduct their research mainly through careful watching of specific films or television series (for an explicit reflection on this research design, see Shepherd, 2012, p. 2). But this emphasis is also due to the type of questions they ask. Weber's analysis of select post-9/11 U.S. movies focuses on the "moral grammars" (Weber, 2005, pp. 10–12) articulated by these films that then percolate into citizens' "imaginary" of the place of America in the world. Similarly, Shapiro (2008) explores the "violent cartographies" expressed in modern U.S. cinema. Macleod (2014) turns the circle even further, innovatively reading two Swedish and Italian "noir police procedural" novel series known by their eponymous detectives, *Wallander* and *Montalbano*, as a new paradigm for critical security scholarship itself. In contrast, this article follows those works that focus more on tracing popular culture references, styles and themes in political practices. Prince (2009, pp. 74–79) argues that the 9/11 attacks were framed through the prism of earlier dramas featuring burning tower blocks going back to the 1930s, as well as having a clear impact on later films. Stimmer (2019) shows how the term "Star Wars" for Reagan's Strategic Defense Initiative (SDI) shaped advocacy and acceptance of the policy itself (as a former actor, Reagan was an avid consumer of film). The first step in following this research direction is to introduce the relevant popular cultural components: namely, noir and its infusion with science fiction, cyber-punk and other genres.

Noir and cybersecurity

"Noir" is a term applied to several mediums of entertainment and popular culture including films, books, television series and comics. The term itself is often traced to the *series noire* on television in interwar France (Porfirio, 1976, p. 4), while influences on noir include detective novels like Agatha Christie's *Poirot* and Arthur Conan Doyle's *Sherlock Holmes*, the "hardboiled" style of U.S. writers such as Dashiell Hammett and Raymond Chandler, and the "police procedural" genre. The most prevalent use of noir is in the term *film noir*, coined by French critic Nino Frank in 1946, who used "*films noirs*" to describe a specific set of U.S.-made films that travelled to France after the end of World War II (Frank, 1996, p. 21). These films tested the boundaries of Hollywood censors at the time due to their sexual and violent content and "immoral" subjects and messages (Borde & Chaumeton, 1996; Spicer, 2007). The original *films noirs* were followed by a revival in the 1970s commonly termed "neo-noir", which either updated noir characteristics to that time or set their story in the original noir era (Erickson, 1996).

Film scholarship contains significant disagreements about the definition of noir. Its overall status as a genre is often questioned, and noir is often described instead as a style, tone or mood (Palmer, 1996, pp. 14–17). Some analyses focus on formal and content characteristics (chiaroscuro effects, voiceovers, retrospective narratives, casting types), and view various directors' idiolects as part of the noir movement (Porfirio, 2013). Other scholars divide definitional strategies for film noir into semantic approaches, which catalogue core elements, and syntactic approaches, which trace relationships between films (Bould, 2005, p. 6). The relationship between popular concepts of noir and the noir canon is complicated: for example, despite the close mixing of popular and classical musical styles in early noir, cool jazz is now a signifier of noir itself (Ness, 2008, p. 69). Overall, Naremore (2008, p. 254) argues for conceptualizing noir as a discourse rather than a genre. In his words:

> [noir] belongs to the history of ideas as much as to the history of cinema … it has less to do with a group of artefacts as with a discourse – a loose evolving system of arguments and readings that help to shape commercial strategies and aesthetic ideologies. (p.11)

Importantly, noir has unconventional moral features. As Naremore (2013) notes, noir is unusual because of "its anti-utopian qualities … ; its disorienting narratives; its mesmerizing play of style; and its complex treatment of gender, sexuality, and race." Walker-Morrison (2018, pp. 4–5) lists five key noir themes: crime, greed and eroticism; a somber tone; pessimism, fatalism and angst; moral ambiguity; and an absence of positive closure. Consequently, unlike the television series examined by Shepherd (2012, p. 4) that provide "order, metaphysical significance, and certainty" to their viewers, noir narratives do not have simple divisions between "good guys" and "bad guys" or a clear moral message concerning their dark subjects of crime, violence, and angst. The overall narrative arc is not one of restoring order, but is instead a constant chaotic, violent and unfair world. It should be noted that some scholars argue that noir amorality only occurs in context of the failed projects that are socially unacceptable (Palmer, 1996, p. 12); consequently, their failure itself suggests that "conventional" morality remains the standard by which these characters are judged. Others highlight the refuges and small moments of hope in noir films, especially optimistic relationships of trust despite evidence to the contrary (Hallberg, 2015). Nonetheless–and crucially for my purposes–the aesthetics and moral tone of noir are intimately linked: a darkened, somber aesthetic reinforces the moral ambiguity of noir characters. I will return to this association in the following sections when analyzing cybersecurity expert practices.

As indicated in the previous section, the integration of noir elements into cybersecurity, as an interaction between two discourses, calls for a post-structural analysis. Post-structuralism holds that discourses are fluid and historically contingent systems of signification (Hansen, 2006; Milliken, 1999). As Hansen (2006, pp. 19–28) outlines, this means that discourses are constitutive of reality, so there is no extra-discursive facts to which discursive representations can be compared, and are plural, so there are multiple discourses in any area of analysis, with the focus and limits partly decided by the observer with their own interests and strategies. Consequently, a useful way of understanding relationships within and between discourses is through the concept of "intertextuality": the appearance of elements of one text in another, and more widely the myriad intricate relationships between different texts (Derian & Shapiro, 1989). If both popular culture artefacts and political representations are texts (in the broadest possible sense of the term as something with meaning), then intertextuality highlights the two-way relationship between them. Political characters, stories and tropes are recognizable in popular culture, and vice versa.

The starting point for understanding noir influences in cybersecurity expert discourses is the relationship of noir to other areas of popular culture, especially science fiction. Cybersecurity, unsurprisingly, has many science fiction elements and prominent early descriptions of cyberspace resembled or were science fiction, such as *Neuromancer* (Barlow, 1996; Gibson, 2003). Other science fiction films, especially 1983's *War Games,* were key influences on U.S. policy, including in the creation of the U.S. Computer Fraud and Abuse Act (Kaplan, 2017). Noir has entwined repeatedly with science fiction in cinema, especially through adaptions of the stories of Philip K. Dick. These include Ridley Scott's *Blade Runner* (1989), which was based on the short story "Do Androids Dream of Electric Sheep?," mixing mid-twentieth century aesthetics with artificial intelligence and humanoid "replicants", as well as *Total Recall* and *Minority Report*. For Zizek, in a piece examining the epistemological anxieties of noir protagonists, noir "realizes its notion only by way of its fusion with another genre, specifically science fiction or the occult" (Zizek, 1993, p. 200). A significant dystopian strand of science fiction–often labelled "cyber-punk"–is thus not easily distinguishable from noir, and Luhr (2012) has gone as far to label the *Terminator* films and *Minority Report* as "tech noir"(p.47). Other notable fusions include *The*

Matrix trilogy and *Ghost in the Shell*, while more recent television series such as *Mr. Robot* and *Black Mirror* continue this trend.

The figure of the hacker illustrates how this intersection between science fiction and noir includes both aesthetic and moral elements. The concept of a hacker is foundational in cybersecurity, stretching beyond lone or socially marginalized individuals with unusual skills. Nissenbaum argues that legislative bodies and media have inverted a valorized view of creative individuals who sought ways around the technical constraints of the early architecture of the internet, with hackers instead becoming outlawed as "terrorists of the Information Age" (Nissenbaum, 2004). Other authors show how such perceptions incorrectly homogenize hacker communities (Coleman, 2014; Coleman & Golub, 2008), especially through gender stereotypes (Tanczer, 2016). Popular culture is a crucial aspect of this representation. The hacker stereotype itself originates in several strands of popular culture (Wall, 2008), while some hacker groups have adopted sophisticated media practices (Kubitschko, 2015). Overall, a dominant association with transgression and danger makes hacker images a rich repository for noir influences, despite the "diverse repertoire of moral genres" potentially available in "hacker morality" (Coleman & Golub, 2008, p. 271). I return to such images in the following section.

Another relevant perspective on the joint influence of noir and science fiction on politics is offered by cultural theorist Baudrillard, whose writings reference many of the works above, and include a sustained analysis of the dystopian *Crash,* the novel by J.G. Ballard and film by David Cronenberg. Claims that mass media have created an environment where events are mediated and *re*-presented to such an extent that one can no longer sensibly speak of a real event or model to which the representations refer; this is the meaning of his famous formulation that the Gulf War "did not take place" (Baudrillard, 1995). We exist instead in the "hyperreal," where the distinction between simulation and reality has collapsed, and signification does not require a pretense to origin and authenticity (Baudrillard, 1994). Baudrillard was himself an influence on the works above; for example, *The Matrix* includes a shot of a hollowed-out copy of Baudrillard's *Simulacra and Simulation*. As McQueen recounts in his analysis of Baudrillard's relationship to the cyber-punk movement, Baudrillard's sneering response was that "*The Matrix* is the kind of film about The Matrix that the Matrix itself could have produced" (McQueen, 2016, p. 6). Snide remarks aside, Baudrillard's work on simulation has striking resemblances to the problems facing the legitimate/malicious distinction discussed in the first section of this article. In *Simulacra and Simulation,* he explains the primacy of simulacra as follows:

> How to feign a violation and put it to the test? Go and simulate a theft in a large department store: how do you convince the security guards that it is a simulated theft? There is no "objective" difference: the same gestures and the same signs

> exist as for a real theft; in fact the signs incline neither to one side nor the other. As far as the established order is concerned, they are always of the order of the real. (Baudrillard, 1994, p. 20)

This paragraph neatly encapsulates the dilemma of cybersecurity experts in distinguishing between legitimate and malicious activity, faced with social structures that permit penetration testing, bug bounties, and defensive tools that are *exactly* identical to those used offensively. In such a situation, Baudrillard argues that "the web of artificial signs will be inextricably mixed up with real elements" (Baudrillard, 1994, p. 20). Consequently, any value orientation towards the true or real is lost, resulting in a world devoid of moral compass, because "hyperreality and simulation are deterrents of every principle" (Baudrillard, 1994, p. 21). Baudrillard's ideas thus provide further underpinning for the moral ambiguity and disorientation suggested by the science fiction, cyber-punk and noir genres above. However, Baudrillard's analysis is conducted at too abstract a level for useful insights into the everyday practices of cybersecurity experts. Although he claims to eschew grand narratives, a pessimistic–and deliberatively provocative–grand narrative is exactly what is offered (Chen, 1987; Lundborg, 2016). In the next sections, I examine the influence of noir at a more concrete level, delving in turn into the visual styles and naming conventions of cybersecurity expert discourses.

Following Hansen's (2006, p. 66) tripartite distinction between official, semi-official (what she calls "wider foreign policy"), and popular texts, I examine semi-official texts produced by cybersecurity experts. The concept of expertise plays a crucial role in cybersecurity, and cybersecurity experts range from public cyber "gurus" to those that channel their expertise more directly, and less overtly, towards customers and clients (Shires, 2018). Although these texts are primarily factual reports, as Shepherd suggests, "even mechanistic, scientistic accounts and 'factual forms of knowledge' rely on narrative form and content" (2012, p. 3), and so the metaphors, analogies and other rhetorical and aesthetic elements of these texts are amenable to analysis (Betz & Stevens, 2013). However, I do not neatly divide governments from "corporate institutions" in the manner of Hansen's (2006, p. 61) methodology. Most cybersecurity experts have experience on both sides (and some former hackers are experts independent of any institution), and so texts ostensibly by corporate authors, or by dedicated cybersecurity news websites and blogs, can carry the stylistic marks and authority of official texts. Finally, the question of technology requires a further qualification. As Dunn Cavelty and Balzacq (2016) demonstrate, technologies are also authors in cybersecurity expert discourses, as both software and hardware are able to represent–to write–as well as be represented. The affordances of these technologies shape cybersecurity expert discourses in several ways, by constraining the form and circulation of reports and by generating content of the reports themselves.

Visual styles and images

My focus on cybersecurity images in this section follows what Bleiker (2001) has termed "the aesthetic turn," wherein scholars in security studies have directed their attention to how film, television, and photography portrayed security themes more commonly analyzed in narrower terms of text and speech. Although the aesthetic turn includes many of the popular culture analyses referenced so far, some scholars in critical security studies focused more narrowly on the role of *images* in international politics, rather than the visual world generally (e.g., Andersen, Vuori, & Guillaume, 2015; Heck & Schlag, 2013; Methmann, 2014). These works built on the theoretical apparatus provided by Hansen (2011, 2015), who interpreted controversial Muhammed cartoons and Abu Ghraib photos as "icons" that embodied particular conceptions of security. In this section, I argue that several aesthetic themes established through the interaction between noir, dystopian science fiction, and cyber-punk in the previous section find their way into expert texts in cybersecurity, priming their readers to expect substantial moral ambiguity.

For cybersecurity, the first crucial question is to what extent practices that are, in Andersen and Möller's (2013) terms, "at the limit of visibility" can be incorporated into visual analyses. Due to its relative novelty and digital basis, many concepts and objects in cybersecurity have no obvious visual association, and so even though images are used powerfully in other security domains to frame issues in certain ways, the scope for doing so in cybersecurity is much wider. Consequently, as Hall, Heath, and Coles-Kemp (2015) suggest, many techniques of cybersecurity visualization deserve further critical scrutiny. For example, cybersecurity expert discourses sometimes portray their subject visually though metaphors with analogue security devices, such as padlocks. Cybersecurity company logos, product packaging, and many software programs use padlocks and similar devices to signal cybersecurity, because these images signify security in the physical realm. However, such metaphors quickly break down as these images become incorporated into cybersecurity functions themselves. A padlock symbol on a web browser appears automatically when the secure protocol HTTPS is used, appearing to protect users as well as symbolizing their protection. Here, the complex architecture of certificates and permissions behind HTTPS is reduced to a binary choice between secure/not-secure by the presence or absence of a padlock icon, and consequently is ignored by both experts and non-specialists (Kelley & Bertenthal, 2015). Due to these issues, although analogue metaphors play a role in broader cybersecurity awareness, they are not the main visual representation of cybersecurity in expert texts.

In contrast, in many expert texts cybersecurity is visually portrayed through a variety of symbols that simply indicate invisibility and illegibility, such as binary or hexadecimal code. The green/blue/black aesthetic of these code images has a twin factual and fictional genealogy. On one hand, the first Uniscope computer monitors, developed in the 1960s, were known as "green-screen" terminals due to the colour of the text on their black displays, although later models displayed white text (Brown & Workman, 1976). On the other, landmark images of code in films such as *The Matrix* drew on this aesthetic, using cascading screens of green code to represent an entire virtual reality. The code in contemporary cybersecurity images is indebted to both histories, although–following Baudrillard–the distinction between "real" and "simulated" code is not always clear. Many reports include code from "real" cases in the main body of the text and "illustrative" code on borders and title pages; however, in some cases this "real" code, such as that from the 2010 Flame virus, loses its function as a set of instructions directing the action of particular systems, and instead becomes an "illustration" of generic cyberattacks (Zetter, 2012). Code images are thus multivalent: the same characters could clarify a technical point or illustrate an invisible threat.

Although code images suggest some qualities of cybersecurity–namely as a virtual, technically advanced, non-geographic "space"–cybersecurity geographies are also illustrated in a more direct sense, with a range of visualization software representing real-time databases of cyberattacks. As scholars in conventional military studies have demonstrated, spatial diagrams of conflict exert a powerful influence on professional soldiers, cleansing conflict from unwanted elements such as blood and fear and thereby "making war possible" (Wasinski, 2011). In cybersecurity, "attack map" programs, made by several prominent cybersecurity companies and often available online, are nearly always world maps set on a dark background, with neon flashes between countries indicating malicious communications (Krebs, 2015). These maps all look surprisingly similar, and their design is clearly indebted to noir visual styles. Although they have been criticized for their inaccuracy and sensationalism (one even makes a "pew-pew" sound imitating gunfire), interviews with their users suggests that this misses their main purpose: to advertise to potential customers (Ragan, 2017). Again, the line between illustration and demonstration is unstable. The threshold for inclusion as a data point in an attack map is usually set low, so reconnaissance and scanning activity appears as an "attack." If taken literally, this is a clear misrepresentation of the threat; however, if seen as merely an indicator that cyberspace is a world of constant threat and unidentifiable enemies, its level of detachment from "reality" is a less appropriate question.

The other dominant spatial representation in expert cybersecurity discourses is of cyberspace as a network, without geographic boundaries but with nodes joined and clustered according to common attributes or other definitions of distance (Betz & Stevens, 2013). Many cybersecurity companies offer analysis software that represents cyber threats in a network form. Some of these programs draw directly on noir imagery to populate "threatening" nodes in their network maps. Both open source and proprietary versions have their default visualization of a "threat" node as a cartoon noir character, complete with greatcoat, trilby, and dark glasses (Haskins, 2019; OASIS Cyber Threat Intelligence, 2019). This dark, hatted, figure operates as part of a wider discursive constellation of threat images in cybersecurity. Hats have been part of the cybersecurity discursive landscape since its inception, with "black hat" and "white hat" signaling offensive and defensive actions respectively, and one of the largest cybersecurity conferences named after the former. The black/white hat distinction as moral symbolism is commonly but erroneously traced to 1930s Westerns (Laskow, 2017), and its moral connotations in cybersecurity are so sedimented that a "grey hat" designation is used to identify those that conduct both offensive and defensive action.

The black hat becomes a black hood in the most recognizable noir-influenced cybersecurity visualization, the paradigmatic stock "hacker" image (Figure 1, overlaid with green code). The hacker stock photo reportedly first appeared in 2008 (Know Your Meme, 2016), and images similar to Figure 1 accompany many cybersecurity texts. Such images often include a hood, dark face, balaclava, leather gloves, and keyboard, and clearly borrow significantly from the noir visual style and palette. The discursive power of these images in shaping expert cybersecurity discourses has been noted by IR scholars (Unver, 2017), and they are seen as so detrimental to a "proper" representation of cybersecurity that influential funding bodies have commissioned projects to find a replacement (Sugarman & Wickline, 2019).

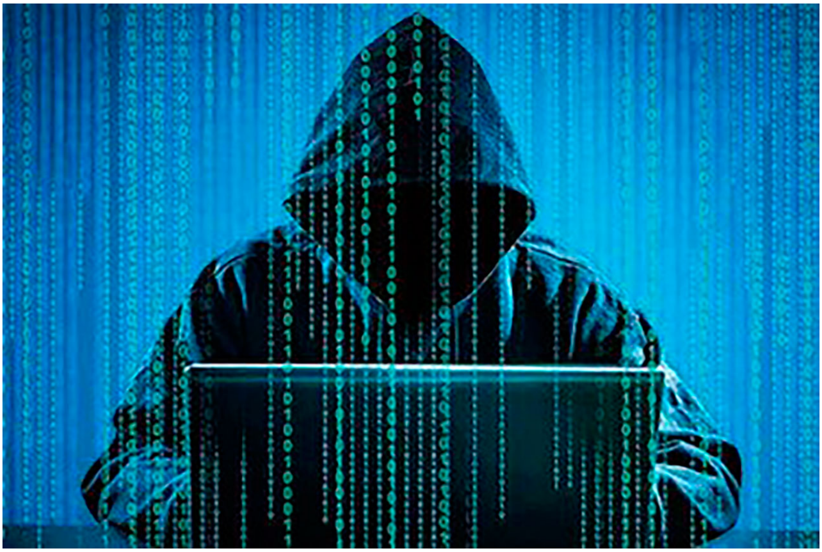

Figure 1. *Hacker stock photo*. Image credit: "hacker-1," iaBeta © 2017, Public Domain.

Although these images populate expert cybersecurity texts, they are designed by commercial artists drawing on their popular conception of cybersecurity, rather than any expert knowledge. As an interview with a photographer who specializes in these photos explains:

> I know nothing about hacking and never have paid any attention to the specifics of it either. It's pure imagination at work here, both mine and the viewer's, who realises the image illustrating an article is just a symbolic supplement to the text. (Cox, 2016)

This "pure imagination" is infused with a noir aesthetic, indicating that the hacker stock image owes more to the lineage of noir films than technical "specifics." This interview also illuminates unexpected technical rationalizations for apparently noir elements; for example, black balaclavas are used to prevent facial recognition of the photographer's model and any automated association with illegal activity. Although the photographer's phrase "symbolic supplement" is exactly right, he downplays its influence, claiming that images are "just" an accompaniment to text. In fact, noir images are also used by hackers themselves, *becoming* the threat that they are perceived to be. For example, the Anonymous hacker collective uses two images: the image of a suited figure with a question mark replacing the head, signifying anonymity, or a mask with stylized depiction of Guy Fawkes from the noir graphic novel and film *V for Vendetta* (Coleman, 2014, p. 64).

The interaction between offensive, "black hat," cyber actors and noir visual styles can be even more complex, as illustrated by the group "Shadow Brokers," known for their leak of U.S. National Security Agency (NSA) hacking tools in 2016 and 2017 and reportedly associated with the Russian state (Schneier, 2017). The Shadow Brokers themselves did not provide any prompts for their visual persona, with their online accounts featuring only text or empty profile images. Despite this blank canvas, extensive noir imagery emerged in reports of this group, with widespread images containing dark silhouetted figures in overcoats and fedoras against a red background (Kumar, 2017). Although the name "Shadow Brokers" echoes a set of characters from fantasy game *Mass Effect*, this reference was quickly overtaken by the noir imagery, originally created by cybersecurity news website The Hacker News. Other texts identified further visual connections between different cyber threats, with another tech news site suggesting that the Shadow Brokers' NSA leak "was meant to *look* like it was carried out by Guy-Fawkes-mask-wearing ideological warriors" (Templeton, 2016). This multi-layered description again dissolves neat distinctions between "real" and "simulated" threats, as it links the Shadow Brokers to Anonymous *specifically* through their visual style, despite recognizing the artifice of the Shadow Brokers identity.

Finally, despite the prevalence of the classic hacker stock image and its derivatives, these classic noir influences are not the only depictions of threat actors in cybersecurity. Other images connoting violence and death, such as a skull and crossbones or devil horns (and even the devil emoji), feature prominently in cybersecurity visual styles. As attribution capabilities in both states and the private sector have grown, stock images have been replaced by traditional mugshots, stills from webcams, and images from court appearances. In particular, the threat intelligence industry has honed its imagery, influenced by the sophisticated cartoon style of graphic novels and films like *Sin City* and *Se7en*. For example, Fancy Bear, the codename for a Russian threat actor invented by cybersecurity firm Crowdstrike, is portrayed on all their reports with glowing red eyes and a Soviet-style fur hat (Crowdstrike, 2019).

Overall, visual styles and images in cybersecurity expert discourses play a key role both in constructing specific entities and in shaping the overall cybersecurity field itself. Through code images signifying illegibility and technical sophistication, and pseudo-geographic "attack maps" emphasizing constant threat, cybersecurity is portrayed as a dark and uncertain world where simulation slips easily into reality and reality into simulation. A range of threatening identities are created using images of noir characters, various coloured hats, and hooded hackers. These images and visual styles use noir aesthetics and palettes to convey transgression, danger and moral ambiguity. In the next section, I turn from visual styles to textual representations to explore how such morally ambiguous identities enable expert practices that embody this transgression and liminality.

Names and practices

One of the most obvious features of cybersecurity expert discourses is that it is full of new proper nouns. Individuals, corporations, hacking collectives, threat actors, even specific vulnerabilities, exploits and hacking tools all have their own pseudonyms, *noms de guerre*, handles and codenames. Cybersecurity experts do not create nomenclature from nothing, and these names are infused with popular culture, through direct references and quotations and in their style, sound and visual aspect.

Many names evoke the crossover between noir, science fiction, fantasy and cyber punk in popular culture. The UK's counterpart to the NSA, the General Communications Headquarters (GCHQ), uses codenames that display a range of "geeky" humor infused with science fiction (Hern, 2014). Such references include graphics novels-films such as *Deadpool* and *X-Men*, and even a technique for obtaining the IP address of MSN messenger users called "Photon Torpedo," from the *Star Trek* weapon (The Intercept, 2014). The U.S. government is similarly indebted to science fiction: the Department of Defense (DoD) cloud migration project, started by a Defense Digital Service team that wear hoodies and embrace counterculture, is named "JEDI"

(Garamone, 2016), while the same team were prevented from using another *Star Wars* reference because DoD seniors viewed "C3PO" as a "stupid acronym" (Bandler, Tsui, & Burke, 2019). The names of cybersecurity companies continue this theme. A leading surveillance and data analysis company is called Palantir, the name of the "seeing-stones" in *Lord Of The Rings*, while even companies without explicit references evoke a similar atmosphere, in words like FireEye, Crowdstrike, Crysys, and Cylance. They pass on these connotations to their proprietary platforms: for example, Crowdstrike's intrusion detection software is named Falcon, evoking not just the bird but also the *Star Wars* spacecraft of the same name. Although these are clearly strategic marketing decisions–it is easier to convince a customer of the purpose of a Falcon than to explain the technical details of its function–they also shape the identity of the individuals who work in these organizations and the organizations themselves.

Names do not only shape identities on the defensive side of cybersecurity expert discourses. "Threat actors"–combinations of technical signatures, behavior patterns, and operator identities–are given codenames by every cybersecurity company that investigates them, leading to a proliferation of names lamented by most experts. These choices are part threat construction, part branding, and part knowing in-jokes, and they are selected just as often by the analysts themselves as they are chosen by marketing departments. Specific vulnerabilities also receive names that could be straight from dystopian fiction, like "Heartbleed," "Spectre," "Meltdown," and "Rowhammer." Often, threat names depend on a close familiarity with the technological objects of cybersecurity. Specific malware strings, drive and file names, and internet protocols all make their way into names of cybersecurity threats. Hackers and intelligence agencies also leave traces of names in the software they write; in another scene reminiscent of Baudrillard, it is the reader's task to ascertain whether these are "real" names left accidentally, or if they are a "false flag" simulating the identity of another actor to distract and misdirect investigators (Bartholomew & Guerrero-Saade, 2016). Overall, according to one author, cybersecurity experts:

> … use fancy names and naming schemes that create an emotional, figurative or mythological context. They shed a different light on our work — the tedious investigation tasks, the long working hours, the intense remediation weekends and numerous hours of management meetings. If the adversary is Wicked Panda, Sandworm or Hidden Cobra, we perceive ourselves as some kind of super heroes thwarting their vicious plans. These names create an emotional engagement. (Roth, 2018)

This emotional and figurative context is exactly the kind of discursive interaction expected by post-structuralist approaches. Names with popular cultural influences and narratives not only enliven the working day for cybersecurity experts, but constitute the moral orientation of their world. However, most cybersecurity names do not evince grand superhero narratives. Instead, they highlight a darker aesthetic and more ambiguous moral position. For example, in a textual incarnation of the noir palette explored in the previous section, cybersecurity companies labelled severe vulnerabilities exploited by U.S. intelligence agencies "Black Lambert" and "Eternal Blue," while "Black Energy" and "Grey Energy" are well-known Russian-attributed cyber-attacks. The company names quoted in the introduction also exhibit this preference for noir-inflected colours. Although light and dark shades are classically associated with good and evil, in cybersecurity–as in noir–both "good" and "bad" entities occupy the same place in the visual spectrum. Names thus offer no indication of moral position, deliberately collapsing the fragile distinction between legitimate and malicious activity.

Some names refer more directly to practices that blur the boundary between legitimate and malicious activity, such as the cybersecurity company [redacted]. [redacted] is run by a former Facebook and NSA employee, who "describes himself as a specialist in 'hacking,' 'breaking stuff,' and 'doing impossible things'" (Schmidle, 2018). The choice of [redacted] as the name for this cybersecurity company discreetly emphasizes the founder's intelligence background by mimicking national security redactions from official documents. But the echoes travel further and become more distorted as they do so: in a postmodern flourish, the company advertises its lack of a name by making its erasure especially prominent. Consequently, [redacted] not only implies secrecy but also (in an entirely transparent manner) invisibility, suggesting that a company with no name has more latitude to engage in hacking–as its founder does–than one which follows the traditional corporate confines of a capitalized proper noun. A less subtle example from the same text also points towards transgressive practices. Rendition Infosec, also run by a former NSA employee, refers to one of the most controversial practices of the U.S. War on Terror. Although Rendition Infosec and similar companies reportedly "dance at the limits of computer trespassing every single day of the week" (Schmidle, 2018), rather than transport detainees for torture and interrogation, their deliberate reference to extraordinary rendition signals their willingness to go beyond mere defensive protection for their clients.

More established figures in the cybersecurity industry also combine noir-influenced identities with acceptance of transgressive practices. In his testimony to the House of Representatives sub-committee on cybersecurity in 2013, Kevin Mandia, a cybersecurity CEO and former U.S. government official, emphasized that "cyber remains the one area where if there is a dead body on the ground, there is no police you call who will run to you and do the forensics and all that" (Committee on Homeland Security, 2013, p. 41). This was of course a metaphor, as there was no literal dead body in the Chinese cyber-espionage cases his company were known for. Nonetheless, he portrayed his role exactly like the start of a film noir: an absent police presence, a violent act and a dead body, and a self-reliant private investigator. In other contexts, Mandia indicates an acceptance of and justification for transgressive action. Commenting on the creation of U.S. Cyber Command in 2018, he suggested that "my gut, just pure gut, not fact based — [U.S. Cyber Command] will probably break the niceties … in cyberspace, everyone else is breaking [laws]" (Shoorbajee, 2018). For Mandia, a cyber-noir identity involves public legitimization of offensive practices that break the law–dismissed as "niceties"–and a "gut" instinct that transgression is pervasive throughout cybersecurity.

Even companies and organizations that do not openly comment on transgressive practices seek to portray themselves as having the potential to engage in them. The name of the largest bug bounty program, HackerOne, explicitly attempts to retain the hacker glamour explored in the previous section while requiring a strictly contractual structure for its participants. Another example is of a U.S.-based cybersecurity company with an office located next to a launderette. When I visited this company, I drew a parallel with the fictional office of a spy agency in the cartoon *Archer*, which draws heavily on noir, with visual styles and character similarities–and sometimes exact plot duplication–referencing the noir canon. My guide, an employee at the company, explained that they were well aware of this similarity, and that when they renovated the office they had requested that the launderette sign remain as an *Archer* reference, despite closing the launderette. Although this company does not publicly claim to "hack back," it does engage in several forms of undercover information gathering, and so the employees saw the morally ambiguous *Archer* location as an appropriate site for their work.

For some cybersecurity experts, noir influences have severe consequences. In 2017, British youth Marcus Hutchins became well-known among cybersecurity experts, following his portrayal as the person who singlehandedly stopped the devastating WannaCry virus that affected the UK's National Health Service. He used a simple domain registration tool to do so, re-registering the command and control domain and so nullifying the malware. For some experts, even this is considered a form of "hacking back" and therefore transgressive (x0rz, 2017). However, Hutchins' fame enabled other cybersecurity experts and U.S. law enforcement to follow a trail of domain names, malware names, and handles on hacker forums, including "ghosthosting," "hackblack," "blackshades," and "blackhole," to the creation of an illegal banking virus named Kronos (Krebs, 2017). Hutchins was arrested months after his public appearance and sentenced to time served in July 2019 for his role in distributing this virus (Whittaker, 2019). As such, his switch between black and white hat – including noir preferences in naming conventions - earned him notoriety as well as fame. Hutchins' case is thus the epitome of the co-constitution between noir aesthetics and transgressive practices explored in this section. As his story illustrates, cybersecurity expert identities are constituted in part through noir references and aesthetics that make hacking back, undercover intelligence collection and participation in "grey" or "black" hacking forums a normal, even necessary, set of activities. Furthermore, noir aesthetics destabilize not only the moral orientation of cybersecurity experts, but even the claim of the field to unproblematic factual knowledge, as both attackers and defenders draw on noir influences to mimic each other in unending layers of simulation and artifice.

Conclusion

The cybersecurity story sees the internet as an environment of persistent threat and potential disaster despite its early hopes; in Chandler's terms, cyberspace is "a world gone wrong" (as cited in Luhr, 2012, p. 15). Severe cybersecurity vulnerabilities result from systemic technological, economic or social deficiencies, including distorted incentives for protection on one hand and black markets for stolen information or new exploits on the other. Into this world enters the cybersecurity expert, with the glamour of a spy and the unconventional smarts and independence of a private eye, "relying on their intelligence, intuition, and sheer nerve" (Luhr, 2012). Whether recruited from intelligence agencies or harboring a hacker past, the cybersecurity expert represents both transgression and redemption. He (usually male) switches between legitimate and malicious activity at a whim.

I have argued in this article that the fragile distinction between legitimate and malicious activity in cybersecurity expert discourses is not merely a question of technological similarities, exacerbated by particular economic and institutional structures. Instead, expert identities *themselves* perpetuate uncertainty over what is legitimate and malicious in cybersecurity. These expert identities are constituted through visual and textual influences from broader discourses of noir in popular culture, including dystopian science fiction, fantasy, and cyber-punk. This identity construction adds to the explicit obstacles confronting cybersecurity experts, suggesting that the task of separating legitimate and malicious is much more challenging than commonly thought. Although cybersecurity experts seek to identify and prevent malicious threats while preserving legitimate activity, the popular cultural aspects of their practices simultaneously collapse this distinction, undermining their apparent goal.

This analysis has several limitations. Theoretically, it used the meta-step of analyzing cybersecurity in terms of a popular culture analytical category (noir), rather than tracing the influence of specific films or popular culture artefacts. A more detailed study could delineate the way specific artefacts appear in cybersecurity discourses and practices. The empirical data could also be increased through both qualitative and quantitative means.

Quantitatively, a larger set of images would provide more robust evidence for the influence of noir visual styles, while qualitatively, a more systematic discourse analysis of a tightly delineated set of texts could be supplemented by an extended ethnography or interviews.

Other limitations suggest further avenues for research. The article focuses on the United States and United Kingdom as the site for cyber-noir influences. However, following Smolin's tracing of the emergence of "Moroccan noir" in media representations of the Moroccan police (Smolin, 2013), we cannot assume that this would be the same in all world regions, and so the extent to which this analysis can be generalized remains open. Also, this article has set aside the gendered aspects of noir, despite extensive research in film studies on questions such as sexism, misogyny, and space for feminist criticism in the noir canon. Given the gender imbalances of the cybersecurity profession, one of the further contributions of cyber-noir might be to investigate conceptions of masculinity and femininity in cybersecurity beyond a question of sheer numbers.

If noir accurately captures the cybersecurity worldview, then what next? To return to Weber's (2005) definition of moral grammars as "codes or contexts (or both) about the good and the bad that structure narratives of interpretation" (p. 5), reading the moral grammars of noir into expert cybersecurity practices suggests that there is no easy solution. Despite noir's darker elements, a more conventional Hollywood narrative, triumphing over evil and rejoicing in the final scenes, also seems regressive given the range of narrative possibilities opened by noir. Instead, perhaps cyber-noir can remain a major theme of cybersecurity visual styles and professional practices, but tempered by a recognition that noir itself is fiction; *and so too, to some extent, is cybersecurity*. The violence, catastrophe and glamour of cybersecurity is exaggerated, and deliberately so; cybersecurity experts both consciously and subconsciously dissolve borders between fact and fiction, simulation and reality; and the noir elements of cybersecurity provide entertainment for experts, providing not only deeper meaning but also fun and enjoyment. Consequently, just as noir parodies emerged shortly after the beginning of noir itself, so expert cybersecurity discourses could be read not straight-faced, as signs of impending doom, but less seriously as ironic nods to wider popular culture. In short, rather than telling a different cybersecurity story, we can tell *this* cybersecurity story differently.

Acknowledgements

I thank Myriam Dunn Cavelty and the team at the Center for Security Studies, ETH Zurich, for organizing the conference for which this article was written and for their subsequent guidance and encouragement. A later version of this article was presented at the International Studies Association annual conference in Toronto, March 2019, and I thank the participants and audience of that panel and the

ETH conference for their helpful comments. I especially thank Max Smeets, Katharin Tai, the CSP editors and two anonymous reviewers for their close reading and insightful comments.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

James Shires is an Assistant Professor with the Institute for Security and Global Affairs at the University of Leiden, and a non-resident research fellow with the Cyber Project at the Belfer Center for Science and International Affairs, Harvard Kennedy School. He is also a Research Affiliate with the Centre for Technology and Global Affairs at the Department of Politics and International Relations, University of Oxford. He holds a DPhil in International Relations from the University of Oxford, an MSc in Global Governance and Public Policy from Birkbeck College, University of London and a BA in Philosophy from the University of Cambridge.

ORCID

James Shires http://orcid.org/0000-0002-7481-4037

References list

Adler, E., & Pouliot, V. (Eds.). (2011). *International practices*. Cambridge: Cambridge University Press.

Amoore, L. (2007). Vigilant visualities: The watchful politics of the war on terror. *Security Dialogue*, *38*, 215–232. doi:10.1177/0967010607078526

Andersen, R. S., & Möller, F. (2013). Engaging the limits of visibility: Photography, security and surveillance. *Security Dialogue*, *44*, 203–221. doi:10.1177/0967010613484955

Andersen, R. S., Vuori, J. A., & Guillaume, X. (2015). Chromatology of security: Introducing colours to visual security studies. *Security Dialogue*, *46*, 440–457. doi:10.1177/0967010615585106

Balzacq, T. (Ed.). (2010). *Securitization theory*. Oxford: Routledge.

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

Bandler, J., Tsui, A., & Burke, D. (2019). How Amazon and Silicon Valley Seduced the Pentagon [Text/html]. Retrieved from https://perma.cc/G5PK-4753

Barkin, J. S., & Sjoberg, L. (2019). *International relations' last synthesis?: Decoupling constructivist and critical approaches*. New York, NY: Oxford University Press.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved from https://perma.cc/B757-954D

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space cyber war, cyber terror, and risk. *Space and Culture*, *15*, 110–123. doi:10.1177/1206331211430016

Bartholomew, B., & Guerrero-Saade, J. (2016). Wave your false flags! Deception tactics muddying attribution in targeted attacks. *Virus Bulletin Conference*.

Baudrillard, J. (1995). *The Gulf war did not take place*. Translated by P. Patton. Bloomington: Indiana University Press.

Baudrillard, J. (2012 [1994]). *Simulacra and simulation*. Translated by S. F. Glaser. Ann Arbor, MI: University of Michigan Press.

Bendrath, R. (2001). The Cyberwar debate: Perception and politics in US critical Infrastructure protection. *Information&Security*, *7*, 80–103.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *44*, 147–164. doi:10.1177/0967010613478323

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives*, *27*, 63–92. doi:10.1177/03043754020270S105

Bigo, D. (2008). Globalized (in)security: The field and the ban-opticon. In D. Bigo, & A. Tsoukala (Eds.), *Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11* (pp. 10–49). London; New York, NY: Routledge.

Bleiker, R. (2001). The aesthetic turn in International political theory. *Millennium*, *30*, 509–533. doi:10.1177/03058298010300031001

Borde, R., & Chaumeton, E. (1996). Toward a definition of film noir. In R. B. Palmer (Ed.), *Perspectives on film noir* (pp. 59–65). London: G. K. Hall.

Bould, M. (2005). *Film noir: From Berlin to Sin City*. London: Wallflower Press.

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival*, *55* (2), 81–96. doi:10.1080/00396338.2013.784468

Brown, J. A., & Workman, R. S. (1976). *How a computer system works*. New York, NY: ARCO.

Buzan, B., Waever, O., & Wilde, J. d. (1997). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner Publishers.

Campbell, D. (2003). Cultural governance and pictorial resistance: Reflections on the imaging of war. *Review of International Studies*, *29*(S1), 57–73. doi:10.1017/S0260210503005977

Chen, K.-H. (1987). The masses and the media: Baudrillard's implosive postmodernism. *Theory, Culture & Society*, *4*, 71–88. doi:10.1177/026327687004001004

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso.

Coleman, G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*, 255–277. doi:10.1177/1463499608093814

Committee on Homeland Security. (2013). *Cyber threats from China, Russia, and Iran: Protecting American critical infrastructure (Hearing No. Serial No. 113-9)*. Washington, DC: U.S. House of Representatives.

Cox, J. (2016). Think Stock Photos of Hackers Are Cheesy? Blame This Guy. Retrieved from https://perma.cc/Y4NR-ZK2C

Crowdstrike. (2019). Fancy Bear Hackers—Aliases, Targets, & Methods. Retrieved from https://perma.cc/2PYH-NSU7

Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics & International Affairs*, *32*, 411–424. doi:10.1017/S0892679418000618

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access contested: Security, identity, and resistance in Asian cyberspace*. Cambridge, MA: The MIT Press.

Derian, J. D. (2005). Imaging terror: Logos, pathos and ethos. *Third World Quarterly*, *2*, 23–37. doi:10.1080/0143659042000322883

Derian, J. d., & Shapiro, M. J. (eds.). (1989). *International/intertextual relations: Postmodern readings of world politics*. Lexington, MA: Lexington Books.

Dunn Cavelty, M. (2008a). *Cyber-security and threat politics*. London: Routledge.

Dunn Cavelty, M. (2008b). Cyber-terror—Looming threat or Phantom Menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*, 19–36. doi:10.1300/J516v04n01_03

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*, 105–122. doi:10.1111/misr.12023

Ellis, R., Huang, K., Siegel, M., Moussouris, K., & Houghton, J. (2018). Fixing a hole: The labor market for bugs. In H. Shrobe, D. L. Shrier, & A. Pentland (Eds.), *New solutions for cybersecurity* (pp. 129–159). Cambridge, MA: MIT Connection Science & Engineering.

Erickson, T. (1996). Kill me again: Movement becomes genre. In A. Silver, & J. Ursini (Eds.), *Film noir reader* (pp. 307–330). New York, NY: Limelight.

Fidler, M. (2015). *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis* (SSRN Scholarly Paper No. ID 2706199). Retrieved from Social Science Research Network website: https://papers.ssrn.com/abstract=2706199

Flyverbom, M., Deibert, R., & Matten, D. (2017). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, doi:10.1177/0007650317727540

Frank, N. (1996). The crime adventure story: A new kind of detective film. In R. B. Palmer (Ed.), *Perspectives on film noir* (pp. 21–24). London: G. K. Hall.

Garamone, J. (2016). Defense Digital Service Chief Brings Private-Sector Expertise to Job. Retrieved from https://perma.cc/BU4T-Y8A6

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense. *Defense, and Deception in Cyberspace. Security Studies*, *24*, 316–348. doi:10.1080/09636412.2015.1038188

Gibson, W. (2003). *Burning chrome*. New York, NY: Harper Voyager.

Guzzini, S. (2000). A reconstruction of constructivism in international relations. *European Journal of International Relations*, *6*, 147–182. doi:10.1177/1354066100006002001

Hall, P., Heath, C., & Coles-Kemp, L. (2015). Critical visualization: A case for rethinking how we visualize risk and security. *Journal of Cybersecurity*, *1*, 93–108. doi:10.1093/cybsec/tyv004

Hallberg, R. V. (2015). *The Maltese falcon to body of lies: Spies, noirs, and trust*. Albuquerque, NM: University of New Mexico Press.

Hansen, L. (2006). *Security as practice: Discourse analysis and the Bosnian War*. New York, NY: Routledge.

Hansen, L. (2011). Theorizing the image for security studies: Visual securitization and the Muhammad cartoon crisis. *European Journal of International Relations*, *17*, 51–74. doi:10.1177/1354066110388593

Hansen, L. (2015). How images make world politics: International icons and the case of Abu Ghraib. *Review of International Studies*, *41*, 263–288. doi:10.1017/S0260210514000199

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*, 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x

Haskins, C. (2019). Revealed: This Is Palantir's Top-Secret User Manual for Cops. Retrieved from https://perma.cc/R7ZD-RRQK

Heck, A., & Schlag, G. (2013). Securitizing images: The female body and the war in Afghanistan. *European Journal of International Relations*, *19*, 891–913. doi:10.1177/1354066111433896

Hern, A. (2014). What GCHQ's geeky and misogynistic code names tell us about its coders. *The Guardian*. Retrieved from https://perma.cc/RQS9-CBEQ

The Intercept. (2014). *JTRIG Tools and Techniques*. Retrieved from https://perma.cc/8ZEV-UB4Q

Jones, C. W., & Paris, C. (2018). It's the end of the world and they know it: How dystopian fiction shapes political attitudes. *Perspectives on Politics*, *16*, 969–989. doi:10.1017/S1537592718002153

Kaplan, F. (2017). *Dark territory: The secret history of cyber war*. New York, NY: Simon & Schuster.

Kelley, T., & Bertenthal, B. (2015). *Tracking Risky Behavior On The Web: Distinguishing Between What Users "Say" And "Do"*. Presented at the International Symposium on Human Aspects of Information Security & Assurance (HAISA), Mytilene, Greece.

Kello, L. (2019). Private sector cyberweapons: An adequate response to the sovereignty gap? In H. Lin, & A. Zegart (Eds.), *Bytes bombs and spies: The strategic dimensions of offensive cyber operations* (pp. 357–378). Washington, DC: Brookings Institution Press.

Kiersey, N. J., & Neumann, I. B. (Eds.). (2013). *Battlestar galactica and international relations*. New York, NY: Routledge.

Know Your Meme. (2016). Hacker Stock Photos. Retrieved from https://perma.cc/9JE4-PAU5

Krebs, B. (2015). Who's Attacking Whom? Realtime Attack Trackers. Retrieved from https://perma.cc/U7VX-UXCE

Krebs, B. (2017). Who Is Marcus Hutchins? Retrieved from https://perma.cc/2N53-MSWJ

Kubitschko, S. (2015). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence*, *21*, 388–402. doi:10.1177/1354856515579847

Kumar, M. (2017). Shadow Brokers Group Releases More Stolen NSA Hacking Tools & Exploits. Retrieved from https://perma.cc/68QE-65S9

Laskow, S. (2017). The Counterintuitive History of Black Hats, White Hats, And Villains. Retrieved from Atlas Obscura website: https://perma.cc/7VRH-8KRW

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*, 86–103. doi:10.1080/19331681.2012.759059

Lee, R. M., & Rid, T. (2014). OMG cyber! *The RUSI Journal*, *159*(5), 4–12. doi:10.1080/03071847.2014.969932

Libicki, M. C. (2010). *Conquest in cyberspace: National security and information warfare*. New York, NY: Cambridge University Press.

Luhr, W. (2012). *Film noir*. Chichester: Wiley-Blackwell.

Lundborg, T. (2016). The virtualization of security: Philosophies of capture and resistance in Baudrillard, Agamben and Deleuze. *Security Dialogue*, *47*, 255–270. doi:10.1177/0967010615625474

Macleod, A. (2014). The contemporary fictional police detective as critical security analyst: Insecurity and immigration in the novels of Henning Mankell and Andrea Camilleri. *Security Dialogue*, *45*, 515–529. doi:10.1177/0967010614543584

McQueen, S. (2016). *Deleuze and Baudrillard: From Cyberpunk to Biopunk*. Edinburgh: Edinburgh University Press.

Methmann, C. (2014). Visualizing climate-refugees: Race, vulnerability, and resilience in global liberal politics. *International Political Sociology*, *8*, 416–435. doi:10.1111/ips.12071

Milliken, J. (1999). The study of discourse in international relations: A critique of research and methods. *European Journal of International Relations*, *5*, 225–254. doi:10.1177/1354066199005002003

Musgrave, P. (2019). IR Theory and 'Game of Thrones' Are Both Fantasies. Retrieved from https://foreignpolicy.com/2019/05/23/ir-theory-and-game-of-thrones-are-both-fantasies/

Naremore, J. (2008). *More than night: Film noir in Its contexts*. Berkeley: University of California Press.

Naremore, J. (2013). Foreword. In A. Spicer, & H. Hanson (Eds.), *A companion to film noir* (pp. xix–xxx). Malden, MA: Wiley-Blackwell.

Ness, R. R. (2008). A lotta night music: The sound of film noir. *Cinema Journal*, *47*(2), 52–73.

Neumann, I. B., & Nexon, D. H. (eds.). (2006). *Harry potter and international relations*. Lanham, MD: Rowman & Littlefield Publishers.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*, 195–217. doi:10.1177/1461444804041445

OASIS Cyber Threat Intelligence. (2019). Defining Campaigns vs. Threat Actors vs. Intrusion Sets. Retrieved from https://perma.cc/475Q-EZKG

Paletta, D. (2015). Former CIA Chief Says Government Data Breach Could Help China Recruit Spies. *Wall Street Journal*. Retrieved from https://perma.cc/T5L6-GHL8

Palmer, R. B. (Ed.). (1996). *Perspectives on film noir*. London: G. K. Hall.

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security*, *26*(2), 87–102. doi:10.1162/016228801753191141

Porfirio, R. G. (1976). No way out: Existential motifs in the film noir. *Sight and Sound*, *45*(4), 212–217.

Porfirio, R. G. (2013). The Strange case of film noir. In A. Spicer, & H. Hanson (Eds.), *A companion to film noir* (pp. 17–32). Malden, MA: Wiley-Blackwell.

Prince, S. (2009). *Firestorm: American film in the age of terrorism*. New York, NY: Columbia University Press.

Ragan, S. (2017). 8 top cyber attack maps and how to use them. *CSO Online*. Retrieved from https://perma.cc/U5YQ-MKE8

Roth, F. (2018). The Newcomer's Guide to Cyber Threat Actor Naming. *Medium*. Retrieved from https://perma.cc/USH2-NESK

Schmidle, N. (2018). The Digital Vigilantes Who Hack Back. *The New Yorker*. Retrieved from https://perma.cc/X7S8-DQSJ

Schneier, B. (2017). Who Are the Shadow Brokers? Retrieved from https://perma.cc/F8LM-ED5S

Shapiro, M. J. (2008). *Cinematic geopolitics*. New York, NY: Routledge.

Shepherd, L. J. (2012). *Gender, violence and popular culture*. New York, NY: Routledge.

Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*, *6*(2), doi:10.17645/pag.v6i2.1329

Shires, J. (2019). Family resemblance or family argument? Three perspectives of cybersecurity and their interaction. *St Anthony's International Review*, *15*(1), 18–36.

Shires, J. (in press). Ambiguity and appropriation: Cybercrime in Egypt and the Gulf. In D. Broeders (Ed.), *Responsible behaviour in cyberspace*. London: Rowman & Littlefield Publishers.

Shoorbajee, Z. (2018). Playing nice? FireEye CEO says U.S. Malware is more restrained than adversaries. *CyberScoop*, Retrieved from https://perma.cc/MPB4-BVN9

Smolin, J. (2013). *Moroccan noir: Police, crime, and politics in popular culture*. Bloomington, IN: Indiana University Press.

Spicer, A. (ed.). (2007). *European film noir*. Manchester: Manchester University Press.

Stimmer, A. (2019). Star wars or strategic defense initiative: What's in a name? *Journal of Global Security Studies*, Advance online publication. doi:10.1093/jogss/ogz004

Sugarman, E., & Wickline, H. (2019). The Sorry State of Cybersecurity Imagery. *Lawfare*. Retrieved from https://perma.cc/RB6H-YRMP

Sulmeyer, M. (2016). *Michael Sulmeyer on Cyber Security Sex Appeal*. Retrieved from https://perma.cc/5ZC5-QLRL

Tanczer, L. M. (2016). Hacktivism and the male-only stereotype. *New Media & Society*, *18*, 1599–1615. doi:10.1177/1461444814567983

Templeton, G. (2016). The "Shadow Brokers" NSA theft puts the Snowden leaks to shame. Retrieved from https://perma.cc/KM7Q-AMHA

Unver, H. A. (2017). Do trees fall in cyberspace? Retrieved from https://perma.cc/QY54-KCXR

Van Rythoven, E. (2015). Learning to feel, learning to fear? Emotions, imaginaries, and limits in the politics of securitization. *Security Dialogue*, *46*, 458–475. doi:10.1177/0967010615574766

Vuori, J. A. (2010). A timely prophet? The doomsday clock as a visualization of securitization moves with a global referent object. *Security Dialogue*, *41*, 255–277. doi:10.1177/0967010610370225

Walker-Morrison, D. (2018). *Classic French noir: Gender and the cinema of fatal desire*. London: I.B. Tauris.

Wall, D. S. (2008). Cybercrime and the culture of fear. *Information, Communication & Society*, *11*, 861–884. doi:10.1080/13691180802007788

Wasinski, C. (2011). On making war possible: Soldiers, strategy, and military grand narrative. *Security Dialogue*, *42*, 57–76. doi:10.1177/0967010610393550

Weber, C. (2005). *Imagining America at war: Morality, politics and film*. London: Routledge.

Weldes, J. (1999). Going cultural: Star Trek. *State Action, and Popular Culture. Millennium*, *28*, 117–134. doi:10.1177/03058298990280011201

Whittaker, Z. (2019). 'WannaCry hero' sentenced for selling Kronos malware. *TechCrunch*. Retrieved from https://perma.cc/H4GK-UARR

Williams, M. C. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly*, *47*, 511–531. doi:10.1046/j.0020-8833.2003.00277.x

x0rz. (2017). Hacking back considered harmful? *Medium*. Retrieved from https://perma.cc/K8NM-8DZT

Young, K. L., & Carpenter, C. (2018). Does science fiction affect political fact? Yes and no: A survey experiment on "killer robots". *International Studies Quarterly*, *62*, 562–576. doi:10.1093/isq/sqy028

Zajko, M. (2015). Canada's cyber security and the changing threat landscape. *Critical Studies on Security*, *3*, 147–161. doi:10.1080/21624887.2015.1071165

Zetter, K. (2012). Researchers Connect Flame to US-Israel Stuxnet Attack. *Wired*. Retrieved from https://perma.cc/ZH4R-89DZ

Zizek, S. (1993). "The Thing that Thinks": The Kantian background of the noir subject. In J. Copjec (Ed.), *Shades of noir* (pp. 199–226). New York, NY: Verso.