# Offensive cyber capabilities and state violence: three logics of integration

Egloff, F.J.; Shires, J.

*Journal of Global Security Studies*, 0(0), 2021, 1–18
https://doi.org/10.1093/jogss/ogab028
Research Article

# Offensive Cyber Capabilities and State Violence: Three Logics of Integration

**Florian J. Egloff** [1] **and James Shires** [2]

[1]Center for Security Studies (CSS), ETH Zürich, Zürich, Switzerland and [2]Institute of Security and Global Affairs, Leiden University, The Hague, Netherlands

## Abstract

Offensive cyber capabilities (OCCs) are the combination of people, technologies, and organizational attributes that jointly enable offensive cyber operations: the adversarial manipulation of digital services or networks. Most works on OCCs focus on their (de-)escalatory potential in terms of diplomatic tension, instability, or power. This article argues for a re-orientation toward the normatively prior question of their relative *violence*. It asks: how are OCCs integrated into violent state capacities and what are the consequences? The article proposes three *logics of integration* by which OCCs are included in violent state actions, in both repressive and interstate situations. These logics—*substitution*, *support*, and *complement*—weigh the benefits of using OCCs against an adversary *instead of*, *as part of*, and *in addition to* other means of violence, respectively. The article argues that the violence of OCCs depends on two things: first, whether one adopts a narrowly physical or a more expansive definition of violence and, second, which logic of integration governs their use. On a narrow definition of violence, substitutive and supportive uses of OCCs are less likely to be violent than conventional alternatives, and complementary uses of OCCs are not violent at all. On a wider definition, both substitutive and supportive uses of OCCs can lead to more violence than conventional alternatives, while complementary uses of OCCs are highly likely to increase violence overall. Acknowledging the different logics of integration for OCCs, and understanding their violent effects, has important analytical and policy benefits for global security studies.

## Resumen

Las capacidades cibernéticas ofensivas (Offensive Cyber Capabilities, OCCs) son la combinación de personas, tecnologías y atributos organizativos que permiten de manera conjunta las operaciones cibernéticas ofensivas (Offensive Cyber Operation, OCO): la manipulación por parte del adversario de servicios o redes digitales. La mayoría de los trabajos sobre las capacidades cibernéticas ofensivas (OCCs) se centran en su potencial de (des)escalada en términos de tensión diplomática, inestabilidad o poder. En este artículo, se debate la reorientación hacia la cuestión normativamente previa de su violencia relativa. Se pregunta de qué manera las OCCs se integran en las capacidades estatales violentas y cuáles son las consecuencias. En el artículo, se proponen tres lógicas de integración mediante las cuales las OCCs se incluyen en acciones estatales violentas, tanto en situaciones represivas como interestatales. Estas lógicas (sustitución, apoyo y complemento) ponderan los beneficios de utilizar las OCCs contra un adversario en lugar de otros medios de violencia, como parte de otros medios de violencia y además de otros medios de violencia, respectivamente. En el artículo, se sostiene que la violencia de las OCCs depende de dos cosas: en primer lugar, de si uno adopta una definición de violencia estrechamente física o más amplia y, en segundo lugar, de qué lógica de integración rige su

Egloff, Florian J., and James Shires. (2021) Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogab028

uso. Según una definición limitada de violencia, los usos sustitutivos y de apoyo de las OCCs tienen menos probabilidades de ser violentos que las alternativas convencionales, y los usos complementarios de las OCCs no son en absoluto violentos. Según una definición más amplia, los usos sustitutivos y de apoyo de las OCC pueden provocar más violencia que las alternativas convencionales, mientras que los usos complementarios de las OCCs tienen más probabilidades de intensificar la violencia en general. Reconocer las diferentes lógicas de integración de las OCCs y comprender sus efectos violentos tiene importantes beneficios analíticos y políticos para los estudios de seguridad global.

## Résumé

Les cyber-capacités offensives reposent sur une combinaison de personnes, de technologies et d'attributs organisationnels qui permettent conjointement des cyber-opérations offensives consistant en la manipulation adversariale des services ou réseaux numériques. La plupart des travaux sur les cyber-capacités offensives se concentrent sur leur potentiel (dés)escalatoire en termes de tension, d'instabilité ou de puissance diplomatique. Cet article plaide pour une réorientation vers la question normativement prioritaire de leur violence relative. Il s'interroge sur les points suivants: comment les cyber-capacités offensives sont-elles intégrées aux capacités de violence des états et quelles en sont les conséquences? Il propose trois logiques d'intégration par lesquelles les cyber-capacités offensives sont incluses dans les actions violentes des états, que ce soit dans des situations répressives ou interétatiques. Ces logiques—substitution, soutien et complément—évaluent les avantages de l'utilisation des cyber-capacités offensives contre un adversaire, respectivement à la place, dans le cadre et en complément d'autres moyens de violence. L'article soutient que la violence des cyber-capacités offensives dépend de deux choses: d'une part de si l'on adopte une définition de la violence qui se limite à la violence physique ou une définition plus large, et d'autre part de la logique d'intégration qui régit leur utilisation. Si nous considérons la définition réduite de la violence, les utilisations substitutives et en soutien des cyber-capacités offensives sont moins susceptibles d'être violentes que les alternatives conventionnelles et leurs utilisations complémentaires ne le sont pas du tout. Mais si nous prenons en compte une définition plus large, les utilisations substitutives et en soutien des cyber-capacités offensives peuvent toutes deux mener à plus de violence que les alternatives conventionnelles, alors que leurs utilisations complémentaires sont très susceptibles d'accroître globalement la violence. La reconnaissance des différentes logiques d'intégration des cyber-capacités offensives et la compréhension de leurs effets violents ont d'importants avantages analytiques et politiques pour les études sur la sécurité mondiale.

**Keywords:** cybersecurity, violence, logics, offensive cyber capabilities, strategy
**Palabras clave:** seguridad cibernética, violencia, lógica, capacidades cibernéticas ofensivas, estrategia
**Mots clés:** cybersécurité, violence, logiques, cyber-capacités offensives, stratégie

In June 2019, following limpet mine attacks against oil tankers in the Gulf and the shooting down of a United States unmanned surveillance drone, the US Cyber Command[1] conducted a cyberattack against a group that had been tracking shipping for the Iranian Islamic Revolutionary Guard Corps (IRGC),[2] disabling their systems. US President Donald Trump tweeted his apparent calculus of decision regarding a kinetic response: "We were cocked & loaded to retaliate last night on 3 different sights when I asked, how many will die. 150 people, sir, was the answer from a General. 10 minutes before the strike I stopped it" (van Wagtendonk 2019). This public account is supported by later memoirs, most notably that of John Bolton, the former National Security Advisor. According to Bolton, Trump stopped the planned strike—after the planes were in the air—because it was "not proportionate" and would lead to "too many [Iranian] body bags" (Bolton 2020).

While most commentators have focused on the de-escalatory potential of using offensive cyber operations

1 US Cyber Command is a combatant command of the US Department of Defense.
2 The Iranian Islamic Revolutionary Guard Corps is a branch of the Iranian Armed Forces.

(OCOs) to retaliate to non-cyber incidents in terms of diplomatic tension, instability, or power (e.g., Valeriano and Jensen 2019), this article takes Trump's words seriously, focusing instead on the relative *violence* of cyber and non-cyber operations. The difference between a concern for escalation and violence matters: while escalation is often associated with increased levels of violence, skirmishes like this involving drones and cyberattacks with no loss of life or bodily harm demonstrate that this relationship cannot be assumed. In other words, when considering cyber operations, we cannot necessarily conclude that a pattern of escalation is an increase in violence or a pattern of de-escalation is a decrease in violence. Moreover, the question of violence is normatively prior: scholars and policymakers care about escalation primarily *because* of its potential for violence.

This article addresses this gap in the literature by asking: how are offensive cyber capabilities (OCCs) integrated into violent state capacities and what are the consequences for state violence? This question requires a more nuanced understanding of *how* OCOs are violent, involving deeper analysis of various concepts of violence and harm. It also requires a reorientation of the literature focusing on "cyber conflict"[3] toward a broader literature on political violence and the mobilization of violent resources by states, including their selection between violent and nonviolent tactics.

This article distinguishes between OCOs and OCCs. OCCs are the combination of various elements that jointly enable an OCO: the adversarial manipulation of digital services or networks (Peterson 2013). These elements include technological capabilities such as infrastructure for reconnaissance and command and control, knowledge about vulnerabilities, in-house exploits and intrusion frameworks, and open-source or commercial tools. They also include individuals with skills in developing, testing, and deploying these technological capabilities as well as the organizational capacity to perform "arsenal management" and obtain bureaucratic and legal authorities for action (Healey 2016; Slayton 2017; Work 2019). Thus, OCCs are not cyber "weapons" in the sense of a sitting arsenal but rely on organizational, technological, and human investment brought to bear in an ad hoc and highly tailored manner for specific missions (Smeets 2018b; Smeets and Lin 2018). Many states have developed and used OCCs in the last decade, including the United States and its allies.

To better understand how OCCs are integrated into violent state actions, this article proposes three *logics of integration*. These logics—*substitution*, *support*, and *complement*—weigh the benefits of using OCCs against an adversary *instead of*, *as part of*, and *in addition to* other means of violence, respectively. These logics apply across different sites of state violence, including both repressive and interstate situations.[4] This article argues that the relative violence of OCCs depends fundamentally on two things: first, whether one adopts a narrowly physical or a more expansive definition of violence and, second, which logic of integration governs their use. On a narrow definition of violence, substitutive and supportive uses of OCCs are less likely to be violent than conventional alternatives, and complementary uses of OCCs are not violent at all. On a wider definition, both substitutive and supportive uses of OCCs can lead to more violence than conventional alternatives, while complementary uses of OCCs are highly likely to increase violence overall. Consequently, it is not always the case that OCCs are a nonviolent substitution for kinetic action or an "off-ramp" for violent escalation, as the US–Iran example above may suggest. Some uses of OCCs can lead to more, rather than less, violence.

The article is organized as follows. The first section explores the nature of violence in relation to OCCs, noting a division between a narrow and wider view of violence in cyber conflict studies and political violence literature more broadly. The second section introduces the three logics of integration, synthesizing work on the mobilization of resources for violence by states in both interstate and repressive settings. The third section draws on the public record of OCOs to conduct an initial "plausibility probe" of these three logics, classifying notable incidents within these categories. This section is designed not to conclusively test the argument but to show that the theory-building undertaken here is plausible, with further research required to systematically evaluate these propositions. The fourth section investigates the implications of these three logics for state violence on both

3 Cyber conflict and cyber war are terms that are often used in international relations and strategic studies. Cyber war is a state of armed conflict in which cyber operations (defined in the following paragraph above) are used to achieve battlefield aims. Cyber conflict denotes the state of relations between countries that conduct OCOs below the threshold of armed conflict against one another. Some have termed this state of relations as one of "unpeace" (see Kello 2017).

4 In this article, we refer to "interstate" and "repressive" as contrasting "ideal types" of state violence: the former understood as violent actions by one state against another and the latter as violent actions by a state against its own people. As we discuss in subsequent sections, these ideal types are blurred in practice.

narrow and wider definitions, before the theoretical and policy consequences of this argument are considered in the conclusion.

## Offensive Cyber Capabilities and Violence

Strategic studies tend to sideline the concept of violence in favor of more "neutral" analytical terms (Cohn 1987; Thomas 2011). Following this broader trend, key works on cyber conflict give little theoretical attention to the concept of violence. Kello, for example, argues that OCCs create successive levels of instability in the international system. He focuses on the transfer of power and its distribution without interrogating closely the violence of such transfers (Kello 2017). Nye has suggested that a "useful definition of cyber war is hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence" (Nye 2011a, 21). This formulation leaves open whether such effects are *strategically* equivalent, irrespective of their violence, or equivalent in terms of how violent they are. As the US–Iran example indicates, this is an important distinction. In general, the cyber conflict literature asks whether cyber operations are efficacious in achieving particular purposes, not whether they are violent (Gartzke 2013, 49; Farrell and Glaser 2017; Slayton 2017).

In contrast, the large and diverse field of political violence treats violence as its core object of study. Unsurprisingly, the concept of violence has undergone extensive theoretical examination in this field, leading to a bifurcation between "minimalist" and broader concepts of violence (Bufacchi 2005). Baron et al.'s recent review of the literature makes a similar distinction between direct (physical) and indirect (structural, drawing on Galtung, or alternatively psychological) harm: the former is an immediate consequence of an individual act, while the latter is a longer term consequence of an act mediated by social institutions (Baron et al. 2019). Both concepts have generated large and sophisticated research agendas. Scholars using a narrower concept of violence have examined what Gutierrez-Sanin and Wood call "patterns of violence" across historical and geographical contexts (Gutiérrez-Sanín and Wood 2017; Kalyvas 2019), while scholars deploying the broader concept have interrogated a wide range of phenomena, including gender-based structural violence, disciplinary violence in the formation of the state, global economic inequality, and the violence involved in shaping post-human bodies and assemblages (Scott 1999; Harvey 2005; Shepherd 2013; Wilcox 2015).

Some works on OCCs that do consider violence as a central feature of their analysis join the first strand of the political violence literature in treating them as largely nonviolent alternatives to conventional means, based on a narrow, physical (kinetic), and/or lethal definition of violence. Thomas Rid's influential book, "Cyber War Will Not Take Place," relied on a narrowly physical view of violence disassociated from harm or damage: for example, he states that "non-violent cyber attacks *could* cause economic consequences without violent effects that *could* exceed the harm of an otherwise smaller physical attack" (Rid 2013b, 9, emphasis in original; see Rid 2013a for further discussion of his bodily conception of violence). This was especially the case for the *lack* of violence demonstrated by the well-known Stuxnet malware that interfered with Iranian uranium enrichment facilities, discovered in 2010; Denning, for example, suggested that Stuxnet itself presented "less harm and risk than the kinetic weapon" (Denning 2012, 684). Overall, the brief surge in academic works using a physical concept of violence following Stuxnet concluded that OCCs were unlikely to cause destruction on a scale comparable to conventional weaponry. This conclusion arguably still holds. Although state use of OCCs has repeatedly caused extensive disruption with significant economic losses, in each case, systems recovered shortly afterward, albeit with intense effort, and no one died (Buchanan 2020).[5]

A physical view of violence has thus formed the basis for much subsequent research in the field focusing on specific strategic concepts, including deterrence and coercion (Borghard and Lonergan 2017; Harknett and Nye 2017; Gartzke and Lindsay 2018, 2019; Valeriano, Jensen, and Maness 2018). Although Valeriano and Maness' data-rich exploration of cyber conflict claims to offer a "severity scale" of "cyber violence," they do not expand on what they mean by "cyber violence." Furthermore, their scale is one of effects rather than violence: while damage is mentioned on the first rung, later steps are merely "dramatic effect" and "escalated dramatic effect" (Valeriano and Maness 2015, 78–108). The closely related topic of escalation as a result of cyber operations also assumes that cyber capabilities are nonviolent. For example, Libicki compares "the limited risks of cyberescalation with the nearly unlimited risks of *violent* escalation" (Libicki 2012, emphasis added). Overall, even though this literature addresses violence more directly than the works reviewed above, it sees violence predominantly in terms of "spillover" into non-cyber areas of conflict (Lindsay 2017; Kreps and Schneider 2019; Taillat 2019;

5 There are regular reports of the "first" cyber attack–induced death; see, for example, Ralston 2020. Often, upon closer examination, the causality is either missing or cannot be established.

Whyte 2020). For these scholars, OCCs feature mainly within nonviolent repertoires of political action, with the recognition that they have the potential to be physically violent in certain extreme circumstances.

Others have pushed back against this narrow conception, arguing that OCCs are "constitutive of both physical and non-physical, threatened and applied forms of violence" (Brantly 2017, 73).[6] International legal scholars have investigated concepts of violence and harm extensively in relation to the question of whether a cyberattack constitutes a use of force or even an "armed attack" (Durante 2015; Fidler 2016; Barrett 2017). Finlay recommends that "theorists of cyber security should focus on the notion of violence" (Finlay 2018, 359), while Lupovici emphasizes the socially constructed nature of violence in cyberspace, suggesting that "an act is an act of violence if the actors agree that it is so" (Lupovici 2016, 333). Stevens seeks to include the "affective implications of cyber weapons" in his analysis, "which might include feelings of insecurity or fear" (Stevens 2017, 2, 2015, 103–4). Finally, Egloff includes a nonphysical definition of violence to discuss cyberterrorism (Egloff 2021). These scholars suggest that we should consider even nonlethal or nonphysical OCOs as a form of violence, especially those that intentionally cause harm to the affective life of individuals or community values and identities (for an extensive discussion of this wider definition, see Egloff and Shires 2021).[7] Importantly, from this perspective, threats of violence and coercion are themselves violent due to their impact on the affective life and community. Threats of violence create and spread fear and discomfort and, for coercive threats, introduce limits to freedom of action.

This wider definition still excludes some forms of structural violence, such as economic harms created by system-level dynamics in internet governance.[8] These system-level dynamics could include economic incentives for writing vulnerable software or weakening encryption technologies to enable state decryption. Due to this bracketing of structural economic factors, the use of OCCs for economic cyber-espionage is unlikely to be violent even on this wider view, for three reasons.[9] First, economic cyber-espionage often harms organizations rather than humans, especially property (including intellectual property); second, it may not be intended to cause bodily, affective, or community harm, even if it does so accidentally; and third, even if there is an intent to harm, and a subsequent effect, it is not clear that the means by which this occurs is sufficiently proximate. Even so, a wider definition of violence does include forms of political cyber-espionage, particularly when targeting civilians with the intent to repress. We return to the psychological consequences of surveillance in repressive situations in subsequent sections.

Overall, heeding Krause's caution that "our understanding of violence is inextricably tied up in what we think we need to know and why" (Krause 2009, 338), we do not wish to adjudicate here between the narrow and wider conceptions of violence present in the literature. This is especially important as some policy actors, including the International Committee of the Red Cross, have adopted the wider concept while others—such as the Tallinn Manual—stay within a narrower concept (International Committee of the Red Cross 2019; Schmitt 2013). Instead, we seek to make our discussion of logics of integration compatible with both concepts of violence. Thus, we trace the violent implications of OCCs according to both views in the last section of this article.

6 To take Brantly's argument further, it is unlikely to be a coincidence that the two binary distinctions "violent/nonviolent" and "offline/online" are not only coextensive, but also map exactly onto a more fundamental binary of "physical/nonphysical." Challenging a purely physical understanding of violence, as Brantly does, leads to a questioning both of the physicality of the "offline" world and of the presumed lack of physicality of cyberspace (both in terms of its extensive material infrastructures and what Haraway might call its "cyborg" bodily implications) (Haraway 1985). Pursuing this line of thought further is beyond the scope of the article.

7 We do not mean to distinguish sharply between "affective" and "structural" violence, placing them both within what we call a wider or expanded concept, and what Baron et al. (2019) call "indirect" violence. More philosophically, we recognize that affective phenomena do not simply occur within someone's brain and are shaped or even brought into being through societal interaction: in this way, the affective is as much structural as it is agential (see, e.g., Hall and Ross 2015).

8 Internet governance refers to the global governance rules, mechanisms, and institutions that govern the internet (see further in Radu 2019).

9 By phrasing this exclusion of structural economic inequality from the wider definition of violence as a "bracketing," we seek to avoid implying that it is not a reasonable expansion of the concept. Instead, we only argue that it does not appear as a significant theme in the writings of those advocating a wider view in relation to cyber operations (although see Stevens 2015, 116–20). For an overview of how the international political economy is structurally violent, see the various contributions to the special issue of *Review of International Political Economy* 28 (2), 2021, on "Blind Spots in IPE."

We believe that the inevitable introduction of complexity is warranted by the ability to appeal to both sides.

Perhaps unsurprisingly, the choice between the two definitions significantly affects the extent to which OCCs are considered violent. However, we argue that the violence of OCCs also depends on the relevant logic of integration. To anticipate the argument made later: on a narrow definition of violence, substitutive and supportive uses of OCCs are less likely to be violent than conventional alternatives, and complementary uses of OCCs are not violent at all. On a wider definition, both substitutive and supportive uses of OCCs can—but do not always—lead to more violence than conventional alternatives, while complementary uses of OCCs increase violence by causing nonphysical affective and community harms. Before exploring these relationships further, we first turn to the three logics of integration themselves.

## 2. Three Logics of Integration

This section introduces, in the abstract, three logics that we argue govern the integration of OCCs into existing state structures. These logics are *substitution*, *support*, and *complement* and they weigh the benefits of using OCCs against an adversary *instead of*, *as part of*, and *in addition to* other means, respectively. We apply these logics to specific OCOs in the following section.

We use the term "logic" to recall the rich scholarship on various logics of action in international relations, with the common aim being to understand the process by which actors (mainly states) understand themselves, their situations, and possible options and then formulate choices and make decisions (e.g., Fearon 1995; March and Olsen 1998; Pouliot 2008; Hopf 2010). This section also builds on work seeking to apply theories of contentious politics, especially repertoires and logics, to international relations and global security issues (Goddard, MacDonald, and Nexon 2019).

Scholars across international relations and political violence have identified the three logics below in other contexts (e.g., Allen and Martinez Machain 2018; Kalyvas 2019). Some have also identified particular logics in the context of cyber conflict; for example, Lindsay and Gartzke distinguish OCCs as "operational complements" from their substitutive role in coercive action (Gartzke and Lindsay 2018). As such, we do not claim these logics as original. Instead, our intended contribution lies in their application to the violent effects of OCCs. In addition, focusing on logics gives us the ability to talk across these different schools of thought, as well as to policymakers thinking in these terms, as evident, for example, in German strategic thinking (von der Leyen 2015).[10]

These logics are exhaustive and mutually exclusive, in that a single OCC deployment will always be one of substitutive, complementary, or supportive. However, the importance of framing and context of the decisions about using OCCs means that not all actors will see a specific deployment in the same way. As a result, the perception of OCC use within these logics may vary between states and between organizations within a state. Furthermore, these logics treat relevant actors as calculating but not entirely rational. This means that they make strategic ends–means assessments but with bounded rationality in terms of predicting the future, the ability to weigh positive and negative possibilities, and emotive and affective influences (Hall and Ross 2015).

First, *substitution* is the use of OCCs to achieve a desired result instead of an alternative. The key characteristic of this logic is a choice between OCCs and another course of action that would achieve the same effect from the decision-maker's perspective. This substitutive choice is context-dependent; the more tactical the decision space, the more similar an effect must be to be a true substitutive choice. In foreign policy contexts, it is rare that an alternative is not proposed, but whether that alternative is a genuine substitution is also context-dependent (Clark and Reed 2005). Often, alternatives are not actually possible or are proposed in such a way that they appear infeasible. Framing is both part of the decision-makers' understanding and used as a tool of presentation—the two are intimately related (in the context of cyber operations, see Dunn Cavelty 2013; Lawson 2013). Substitution is thus between OCCs and a realistic alternative.

A simple example may help to illustrate the difference between substitutive logics at tactical and strategic levels. In a tactical decision concerning how to open a locked door, substitutive choices might be between physical options, such as picking the lock mechanically, or cyber options enabling remote control of the door via an electronic locking system.[11] The effect, i.e., opening the

10 By "German strategic thinking," we explicitly mean the document referenced in-text, which lays out the strategic guidance for cyber defense in the German Department of Defence.

11 It is worth noting that while this hypothetical example is substitutive, the locked door analogy has been examined (and criticized) extensively as a metaphor for cyber operations themselves. See, for example, Libicki's claim of "no forced entry in cyberspace" (Libicki 2009, xiv) and, more generally, Betz and Stevens 2013.

door, is the same. An example of a strategic decision space would be seeking to introduce doubt for an adversary's leadership over their command and control ability. The substitutive choices offered may entail various physical sabotage and covert action options as well as their cyber equivalents.

Second, *support* is the use of OCCs in service of another course of action. There is nearly always a larger plan for OCC use (even if that plan is deliberate chaotic intention, as in Rid 2020, 329–422) or a wider strategy into which specific OCC deployments fit (Smeets 2018a). The logic of support does not seek to pinpoint a mutual reliance between tactics and strategy (i.e., that tactical actions should always support a strategic objective) but instead dependencies *at a similar level* (some tactical actions support others, just as some strategic actions support others). Supportive uses of OCCs are thus always part of a conflict involving other means and become integrated into broader aims of "war-fighting" (Slayton 2021).

At a tactical level, the aim of OCOs is usually to increase the probability of success of, decrease risks around, or magnify the effects from another course of action (Brantly 2016). Supportive uses of OCCs often seek to counter adversaries' counterstrategies (Healey, Jenkins, and Work 2020). In this way, they function like other "electronic warfare" options, such as jamming, i.e., the deliberate interference with or blocking of an adversary's electromagnetic spectrum, which can support an air raid or other sudden strikes by preventing effective coordination in defense. They can also lay the groundwork for other operations by providing intelligence (Gioe, Goodman, and Stevens 2020). Moving to the strategic level, an early example of strategic supportive use in a military context could be the degrading of essential Georgian services in the 2008 Georgian–Russian war (Deibert, Rohozinski, and Crete-Nishihata 2012).

Third, *complement* is the use of OCCs to achieve a desired result, where no alternative for the effects delivered by OCOs exists. Here, OCOs open a new avenue of action in addition to those that were already proposed or underway, as explored in work on substitutive and complementary uses of air strikes (Allen and Martinez Machain 2018). OCCs can be used in a complementary way alongside the existing means or where there are no other forms of engagement between two adversaries. The desired result is something that is *not achievable* except through OCCs, because OCCs enable new forms of digitally mediated effects.

One example of a complementary use would be the triggering of multiple system failures in various locations simultaneously, spreading unpredictably across adversary networks. Such random, self-propagating disruption is difficult, if not impossible, to achieve without OCCs. A very different example of the complementary uses of OCCs would be the ability to surveil, censor, and intimidate target populations both at a massive scale *and* in a highly targeted manner across international borders. While in both cases these effects are reminiscent of effects that can be caused using conventional means, their scale and character are unique to OCCs.

Before continuing to apply these logics to specific uses of OCCs, we emphasize that in this article, we limit our argument to one specific type of agent: the state. This is a considerable narrowing of the spectrum of political violence more generally. For example, in Kalyvas' classification of eleven forms of political violence, only two (interstate war and repression) are performed by states (Kalyvas 2019). Furthermore, scholars have long argued that non-state actors are relatively empowered by cyber capabilities (e.g., Nye 2011b). On top of this, many forms of violence relevant to OCCs (such as gender-based or intimate-partner violence involving spyware) are not directly associated with the state. Although these are important, we do not consider them here.

We focus on the state because state violence remains, despite the breadth of research above, a foundational form of violence not only in most accounts of OCCs, but also in political philosophy more widely (Frazer and Hutchings 2008; Schinkel 2010). Equally importantly, most states wield physical forms of violence in addition to cyber capabilities, while the set of non-state actors with access to both is far smaller.[12] Consequently, states remain a logical narrowing of scope for this initial exploration, with the potential to expand the analysis in future work. Despite examining only state violence, we nonetheless depart from most works on cyber conflict by adopting the consensus position in the broader literature on political violence that interstate and repressive state violence are part of a single continuum (Davenport 2007; Davenport and Inman 2012).

## Application to Offensive Cyber Operations

This section applies the above three logics to specific OCOs. Before we go into specific cases, a few remarks on our overall methodology are required.

12 At the boundaries, where the distinction becomes blurred, there are on the one hand states without the necessary resources for OCCs and on the other hand large, professionalized, criminal organizations that have good access to OCCs.

## Methodology

Our purpose is to conduct an initial "plausibility probe" of the three logics, as there is not space in this article to conclusively demonstrate their workings. To conduct this initial analysis, we identified cyber operations where the decision-making calculus of the state actor regarding the operations' violent effects plausibly supports each logic. The three logics are therefore initial hypotheses rather than proven phenomena. This method raises several questions around the kinds of empirical evidence we use to make our argument. Hence, in this section, we discuss our data-collection process as well as the status and limitations of our claims.

We draw data from several catalogs of OCOs (see, e.g., Council on Foreign Relations nd; Valeriano and Maness 2015; Roth 2018) as well as independent, open-source research. These catalogs are all published online and are open access, with the first maintained and updated by the Council on Foreign Relations (CFR).[13] These catalogs have developed significantly in the last few years. Early versions focused mainly on incidents, while there has been a more recent shift to thinking of OCOs as campaigns, tracking specific individuals and groups across targets and incidents (Buchanan 2020; Harknett and Smeets 2020; Rid 2020). We adopt this campaign view of OCOs for several reasons. The campaign perspective is better for practitioners, as it enables an understanding of repeated intrusions and development of persistent access and target selection; it is also better for attribution, as it identifies specific groups over time and different forms of activity (Schulzke 2018; Egloff 2020a, 2020b; Egloff and Smeets 2021).

However, we also seek to widen this perspective, thinking not only of OCOs as campaigns but also as part of broader decisions made by states between cyber and non-cyber operations (see, e.g., Gartzke and Lindsay 2019). One of the implications of our argument is that there is no such thing as a purely "cyber" campaign: there are only cyber actions integrated into other actions: intelligence activity, human sources, technical collection, etc., and military force, armies, mercenaries, etc. (cf. Smeets and Chesney 2020).

Given that we seek to build a plausibility probe for our argument, rather than to test it, we selected those campaigns where there are most data available on the distinction between alternative options and their violent consequences. There are, unfortunately, only a limited number of cases where there are sufficient data to make reasonable inferences regarding the decision-making calculus of relevant actors. For example, in the US–Iran cyber operation in the introduction of this paper, both the rare acknowledgement of the operation and the explicit consideration of alternatives enable an analysis in terms of logics of integration and their violent implications. Even in this case, the data are not especially reliable, consisting mainly of Trump's unpredictable tweets and Bolton's personal recollections. Nonetheless, they are better than those available for most cyber operations. While we encourage others to assist us in addressing this data gap more systematically, doing so is beyond the scope of this article.

Our discussion therefore selects on the dependent variable: we only consider cases where OCOs occurred (and are publicly discussed). There is a large set of possible cases where OCCs were considered as an alternative but *not used*. Given that most data are published by defensive actors, we are unlikely to see many of these "negative" cases in the public domain. One example stems from the preparation for the 2003 invasion of Iraq: the United States considered deploying computer network effects to debilitate the Iraqi financial system. However, they decided against it, because of the uncertainty around the consequences of such operations (Markoff and Shanker 2009). Another example stems from the military intervention in Libya in 2011: before the intervention, senior officials in the US government debated whether to disrupt and disable Libyan air-defense systems to protect North Atlantic Treaty Organization (NATO) warplanes. The administration decided not to, as there were uncertainties whether the capabilities would be ready in time, fears that these might set a precedent for Russia and China, and questions around whether the president had the legal power to order such an attack without informing Congress (Schmitt and Shanker 2011). These cases are important to understand "negative" logics of integration—where cyber capabilities are developed but not used—but this is a further research step, and in the ensuing analysis we focus only on "positive" logics.

There is also a set of intermediate cases where OCCs were used for intrusion, but the final stage that could have caused violent effects was not triggered. We are more likely to see these intermediate cases in public reporting—for example, the TRITON malware[14]

13 There are other similar catalogs that are also regularly updated, such as that published by the Center for Strategic and International Studies (CSIS). The CFR database is arguably more useful—although often based on similar or identical sources to the CSIS one—because it treats cyber operations more flexibly in the manner discussed above.

14 TRITON is an attack framework (software) aimed at interacting with specific industrial control systems (built

(FireEye Intelligence 2018)—but the interpretation of such incidents is difficult: it could be testing, a failed attempt at execution, or deliberate signaling that further violence is possible (Buchanan 2020). These interpretive difficulties also arise in cases where violence is clearer, such as NotPetya, discussed below, but the difference is that ambiguities in intermediate cases affect the universe of cases itself (i.e., violent uses of OCCs) rather than the division between different logics within that universe. We, therefore, exclude such intermediate cases from our analysis.

Finally, we exclude instances of state-sponsored cyber espionage for economic purposes, even where there is evidence of the consideration of alternative options, because—as explained earlier—these alternative options are not differently violent on either the narrow or the expanded view of violence. We now discuss specific cases applying the three logics in turn.

## Substitution

The nonlethal and potentially reversible effects offered by OCCs mean that they can be an attractive substitute for conventional means. Besides the cyber operation against the IRGC mentioned in the introduction, where President Donald Trump directly referred to cyber operations substituting for a physical operation, a second cyber operation occurred in response to drone attacks on Saudi Arabian oil facilities in September 2019, which the Secretary of State Mike Pompeo called an "act of war" (Gaouette et al. 2019). In this case, the US targeted Iran's ability to distribute propaganda (Ali and Stewart 2019). Both incidents show how the addition of OCCs enriches the spectrum of *alternative* options in an interstate dispute.

Looking more broadly, Stuxnet, one of the most infamous OCCs targeting an Iranian nuclear-enrichment site, could also be interpreted as a case of substitution (Sanger 2013; Zetter 2014). In this case, instead of using a bunker-buster bomb to destroy the enrichment facility to convince the Iranian leadership of the exceedingly high costs of their nuclear program, the United States and Israel built a piece of malware that degraded centrifuges directly. Of course, this is a simplification of a complex foreign policy choice. The actual choice spectrum on the Israeli side, of which Stuxnet only formed one of a bundle of activities that were designed to convince the Iranian political elite of the bad gain/price ratio of the nuclear program, has been captured well by recent journalistic accounts (Bergman and Mazzetti 2019).

A substitutive logic can also be seen in digital repression. Physical methods of surveillance are often exchanged for digital ones due to the relative ease with which the state can gain access to a person's most private spaces (Asal et al. 2016; Lyon 2018). The attractiveness of OCCs for state surveillance can, for example, be seen in the customer lists of spyware companies such as Hacking Team, FinFisher, or NSO Group (Deibert 2020, 151–60).[15] Software from these companies was a core aspect of authoritarian adaptation in the wake of the Arab Spring, enabling relatively cheap and effective monitoring of journalists, activists, and political opposition in states such as Egypt and the United Arab Emirates (UAE) (Soliman 2020). The role of OCCs as an alternative to more resource-intensive means of gathering information is also evident not only in "successful" post-Arab Spring digital authoritarian states, but also in others' descent into internationalized civil war conflicts. In Syria, repressive practices on all sides included OCCs as an alternative means of surveillance (Scott-Railton et al. 2016).

The substitutive use of OCCs is also evident in other forms of intimidation and repression, in addition to targeted surveillance. OCCs can be used to degrade the capability of political opponents or activist groups by remotely deleting data, rather than physically raiding offices, removing the physical destruction occurring in raids and the violation of physical space by security personnel.[16] Another substitutive use of OCCs for repression is blackmail—a strategy that has historically been used against political minorities (see, e.g., FBI Records nd)—or, more generally, the hacking and leaking of sensitive data (Shires 2019, 2020). For example, Omar Abdulaziz, a Saudi dissident targeted by NSO Group's software, claimed that "more than 30 influencers told me that the Saudi government blackmailed them with

for Triconex Safety Instrumented Systems). It was initially detected in a petrochemical facility in Saudi Arabia in 2017 and later attributed to a Russian research organization.

15 In addition to OCCs as defined in this article, some technologies designed for other purposes, such as quality monitoring or prevention of malware, can also act as substitutes for offline forms of surveillance, especially as states already own them or can justifiably purchase them for benign reasons.

16 The repressive use of OCCs against human rights non-governmental organizations (NGOs) in Egypt has alternated with periods of increased physical repression, including raids and detention of individuals at organizations such as the Egyptian Initiative for Personal Rights.

material obtained by hacking their phones. They were given two options: Tweet propaganda or have your private content, including pictures, released on Twitter" (Kirchgaessner 2020). While blackmail of this kind is not a new repressive tactic, here OCCs clearly substitute for other means of obtaining private data.

### Support

As well as offering an alternative to conventional means, OCCs can also be used in tandem with non-cyber capabilities to achieve violent effects, in what we term a supportive logic. Supportive logics occur where OCCs increase the power, precision, range, or resilience of conventional means. Some cyber conflict scholars have noted this logic in action, including in the cases we discuss below (e.g., Rid 2012, 17; Finlay 2018, 371).

The clearest interstate illustration of supportive logics is where OCCs tip the overall risk calculus of a conventional operation into action. An early example may be cyber capabilities reportedly used by Israel in enabling a 2007 strike on a Syrian nuclear reactor (Adee 2008), though detailed Israeli media investigations do not mention this aspect of the operation, and so there remain reasons to be skeptical of its veracity (Harel and Benn 2018). Some coalition cyber operations against the Islamic State of Iraq and Syria (ISIS) in Syria have supported violent action: as the Director-General of the Australian Signals Directorate (ASD) claimed, "our actions were generated in support of and in coordination with ground manoeuvres" (Burgess 2019). Separately, a US–Israeli cyber operation was blamed for the triggering of Syrian air defense missiles in 2018, but the purpose and details are unclear (Khoury 2018).

Offensive cyber capabilities can also support repression by providing an efficient means to come up with evidence against regime opponents. Access to communications allows the state to know more about what people say and therefore direct other security measures based on speech that otherwise would have disappeared into thin air (Öztürk and Taş 2020). Like other offensive/defensive cybersecurity dynamics, the success of this tactic depends on whether targeted populations also adapt to use more secure methods of communication (Hassib and Shires 2021). At least a decade of research by the Citizen Lab, a Toronto-based academic interdisciplinary laboratory, documents the employment of OCCs that support extrajudicial killings, arbitrary detention, and mistreatment by other elements of the state security apparatus (Deibert 2020).

We can now see in more detail how the distinction between substitutive and supportive uses of OCCs in repressive contexts relies on the separation between tactical and strategic levels discussed earlier. The same spyware used substitutively at a tactical level (e.g., for blackmail above) can in other cases be used supportively, at an equally tactical level. For example, digital surveillance of the contacts of the Saudi dissident Jamal Khashoggi probably played a part in both substitutively motivating *and* operationally supporting his killing by Saudi intelligence officers in the Saudi Embassy in Istanbul (Barnes 2018). However, at a strategic level, both uses are supportive, as they contribute toward a wider aim of suppressing political opposition both within and outside state borders (Michaelsen 2017; Moss 2018).

### Complement

The third logic integrating OCCs into conventional capabilities is as a complementary option in addition to conventional means, expanding states' repertoire of violence. Complementary uses are by far the most common articulation of concerns around the violent effects of cyber operations, by both state and non-state actors (Dunn Cavelty 2008; Gartzke and Lindsay 2017; Futter 2018).

At an interstate level, cyber capabilities can add extra capabilities to intelligence and military action. Some cyber operations against ISIS were complementary; such as the attempts to degrade their media reach in US Operation Glowing Symphony (Martelle 2020).[17] The United States, though there is scant evidence, has also used OCCs as an additional option against Russian media organizations accused of conducting influence operations, often referred to as troll farms (Nakashima 2019). Other frequently discussed complementary uses of OCCs are the North Korean WannaCry ransomware operation that postponed surgeries in the UK National Health Service and the "BlackEnergy" and "GreyEnergy" Russian attacks on Ukraine's energy sector that cut off electricity for a day in winter, thereby potentially endangering human life (Buchanan 2020, 148, 187).

Again, the distinction between complementary and supportive logics is also dependent on the correct identification of tactical and strategic levels of decision. One of the most impactful complementary uses of OCCs is the NotPetya case, where allegedly the main (intelligence) directorate of the Russian general staff (often referred

17 Operation Glowing Symphony was an operation conducted by the US Cyber Command against the ISIS's media operations with the aim to impose time and resource costs upon ISIS and through that to contest the information domain (Martelle 2020).

to by its old acronym GRU) launched destructive malware via Ukrainian tax software that affected a wide range of major multinational firms. At the strategic level, NotPetya may be seen as supportive of a wider Russian destabilization strategy in Ukraine, in the context of the Russian occupation of the Crimean Peninsula and the Donbas region. However, at the tactical level, we classify NotPetya as complementary, because its disruption of the Ukrainian government functions does not appear to have supported specific conventional acts of violence (Buchanan 2020, 288–305).

Complementary uses of OCCs for repression also provide states with additional means for controlling citizens, especially abroad. In contrast to substitutive uses (the replacement of analog with digital surveillance capabilities) and supportive uses (digitally enhanced but otherwise conventional repression), complementary OCCs' use for repression develops *new ways* of applying pressure to or stoking fear in target populations. For example, the Assad Regime-affiliated Syrian Electronic Army's multifaceted campaign targeting multinational media corporations, blackmailing, and extorting other corporations, while conducting defacement, recruitment, and espionage operations, goes far beyond support or substitution (Al-Rawi 2014; Baezner 2017).

Notably, the Chinese government has developed sophisticated means to combine powerful digital surveillance and censorship tools—including OCCs—into new forms of repression, especially against Uighur Muslims in Xinjiang province. The Chinese state's uses of OCCs have included substitutive uses, such as evolving spyware deployed against Tibetan targets over two decades (Dalek, Crete-Nishihata, and Scott-Railton 2016). They have also included supportive uses: Mozur and Perlroth claim that Uighurs were detained for "having two phones or an antiquated phone, arbitrarily dumping a phone, or not having a phone at all," with phone possession probably identified through spyware along with other means (Mozur and Perlroth 2020). However, the sheer extent of the Chinese state's incorporation of OCCs in its efforts to reshape Xinjiang into an economically productive but politically a quiescent province suggests a complementary logic. Most recently, reports of combined social media manipulation, compromised news websites, and malware delivery indicate forms of information control that would not be possible through other means (Dvilyanski and Gleicher 2021).

Overall, these cases suggest that OCCs in all three logics of integration are an increasingly important part of strategic (ex ante) repression, especially motivated by concerns around regime stability (deMeritt 2016; Ritter and Conrad 2016). The final section of this paper considers the implications of these logics for both narrow and wider views of violence.

## The Three Logics and the Theorization of Violence

While the previous section focused only on the different logics of integration for OCCs, this section takes that discussion further, asking whether OCCs are likely to increase or decrease state violence. In doing so, the distinction introduced earlier between narrow (largely physical) and broader definitions of violence is crucial, as the violent effects of OCCs depend on both the definition of violence adopted *and* which logic of integration is involved. To recap, OCCs are largely thought to be nonviolent on the narrow definition, but a broader definition would see many effects of OCCs, especially affective and community harms, as violent in certain contexts. As we believe that the three logics of integration are a useful analytical device whatever definition of violence is adopted, we examine the violent effects of OCCs according to both definitions (table 1). For ease of exposition, in the remainder of this section we systematically address each cell in bold in table 1, in turn.

**Substitution (narrow definition):** A narrow view of violence would suggest that substitutive uses of OCCs are less violent than conventional alternatives. In both the US–Iran cases in 2019 considered above, the alternatives were kinetic actions that would likely have caused more physical and lethal harm. In the case of Stuxnet, the United States' commitment to an OCO helped prevent more harmful action, reassuring Israeli leadership and dissuading more hawkish voices that would have preferred a physical strike. More generally, the aggregate effect of interstate cyber operations on a substitutive logic is likely to be less bodily or lethal violence. A similar argument can be made for repressive contexts, where some bodily harm and physical damage through raids and intimidation are replaced by digital interference with political opposition.

**Substitution (expanded definition):** With an expanded concept of violence, substitutive uses of OCCs relocate, rather than reduce, violent effects. This is because the affective and community-based informational harms caused by OCCs (such as the deletion of NGO data or violations of individual privacy) are also considered violent on this definition. Scholarship suggests that psychological harm, community degradation, and broader chilling effects can, in certain contexts, be as serious as physical harm (Woodlock 2017; Woodlock et al. 2020).

**Table 1.** The Three Logics of Integration and Their Effect on Violence

| Logic | Substitute | Support | Complement |
|---|---|---|---|
| *Summary* | OCCs replace other means of achieving a particular end | OCCs are combined with other means to help achieve that end | OCCs achieve an end not available by other means |
| *Effect on violence (narrow definition)* | **Less violent** | **Less violent** | **Irrelevant** |
| | OCCs achieve the same end without or with less physical harm | OCCs are more precisely targeted, concerns of indirect effects limit use | Complementary effects of OCCs are not physically damaging so not violent |
| *Effect on violence (broad definition)* | **Unclear** | **Unclear** | **More violent** |
| | Affective/community harms could outweigh physical damage depending on context | Affective harms occur even with better targeting, shift in not decreased repression | Affective/community harms caused by OCCs increase levels of violence overall |

Consequently, it is possible that widespread OCOs could inflict affective or community-based informational harms that even exceed physical or material harm—although this is more plausible for repressive situations than for the interstate operations considered above.

**Support (narrow definition):** The supportive use of OCCs is likely to lead to a reduction of violence, narrowly conceived, for two reasons. First, the provision of intelligence and disabling of adversary defenses through OCOs could reduce "collateral damage" from the action the OCO is designed to support. In other words, better preparation for a kinetic strike decreases casualties and lowers the likelihood of failed strikes (Gregory 2015).[18] Second, in an environment where more conventional military assets are increasingly dependent on computer networks, the expectation that adversaries possess OCCs, as well as uncertainty around the indirect effects of cyber capabilities and concerns over lack of control, may constrain the use of both supportive cyber capabilities and conventional means (see, e.g., MacAskill 2017). As mentioned above, there is anecdotal evidence of this approach hindering the supportive use of cyber capabilities in preparation for the 2003 invasion of Iraq.

The supportive use of OCCs could also reduce violent repression, if OCCs enable states to more effectively target leaders of networks. A knowledgeable state—so the thinking goes—is a less-violent state because, even if the violence is equally severe, it is less indiscriminate. Evidence supporting this line of argument is offered by Gohdes, who mapped the differential impact of restrictions on internet communications on targeted versus indiscriminate violence using the narrow definition (Gohdes 2020). Gohdes found that in areas with restrictions on the free exchange of information, violence tended to be more indiscriminate. Importantly, the reverse was true as well: in areas with fewer restrictions on the exchange of information online, violence tended to be more targeted.

**Support (expanded definition):** An expanded definition of violence makes the link between supportive uses of OCCs and a reduction in violence far less clear-cut. For interstate contexts, the precision targeting argument would have to take into account the affective harm caused by constant drone strikes and fear of being targeted, as well as diminishing of community values and identities (e.g., tribal or religious relationships in Afghanistan or Yemen).[19] If concern over digital vulnerabilities in military systems and the difficult-to-control effects of cyber

18 A more nuanced analysis would also consider indirect effects on strike frequency in both directions, following an analogy with lethal autonomous weapons. Strikes with a high probability of failure (i.e., without supporting OCOs) may need to be more frequent to ensure the target is hit. On the other hand, strikes with a lower probability of failure (i.e., with supporting OCOs) may be politically and bureaucratically easier to conduct and so more frequent.

19 For a sophisticated examination of how digital and other technologies support military violence on an expanded definition, see the collection of essays in Suchman, Follis, and Weber (2017). These essays do not explicitly focus on OCCs, but many of their conclusions are relevant to this discussion.

operations leads to overall restraint, then this would also reduce violence even on an expanded definition. In repressive contexts, Gohdes' argument may still hold with an expanded definition of violence. Information controls inflict extensive nonphysical violent harms, and so a lack of such controls would also lead to less affective or community harm, in addition to the reduction in physical violence she has found.

**Complement (narrow definition):** Complementary uses of OCCs are automatically nonviolent in a narrow definition, because they have not—so far—caused bodily harm or death. WannaCry and Black/Grey Energy are the closest examples at an interstate level, as they affected energy infrastructure and hospitals, although public reporting has not revealed bodily harm as a result.[20] The complementary use of OCCs for repression is also nonviolent in a narrow definition, notwithstanding proof-of-concept hacks of personal devices such as pacemakers. This nonviolent yet impactful character of complementary uses has left both scholars and policymakers struggling to capture their impact accurately (Harknett and Smeets 2020).

**Complement (expanded definition):** Many complementary uses of OCCs are violent in an expanded definition. NotPetya is violent, though the exact intent of the attackers matters for the judgment of its severity. On one hand, NotPetya could be seen as the activity of a Russian operational cyber warfare team aimed at eroding confidence in the Ukrainian society, economy, and trust in the defensibility of Ukraine, creating a collective feeling of vulnerability and causing harm at a community level (Greenberg 2019). In this reading, the international indiscriminate effects are collateral damage to the more limited operational intent (the US government appears to subscribe to this view—see White House 2018). A contrasting judgment sees NotPetya's authors as fully culpable for intentionally producing indiscriminate global damage. In this assessment, NotPetya was a carefully considered coercive device for strategic signaling, using the destabilization of global economic actors as a medium to send the message (Valeriano, Maness, and Jensen 2017). We suggest that both accounts are describing violent acts, though the second is more severe than the first as the intent covers a wider area of harm. Complementary uses of OCCs thus increase the level of interstate violence by debilitating the affective lives of individuals and inflicting harm on communities.

20 For WannaCry, the UK government audit affirmed that "NHS organisations did not report any cases of harm to patients" (UK National Audit Office 2018, 14).

Regarding repression, the complementary use of OCCs to create an environment of pervasive censorship and fear, as in Xinjiang, also implies increased violence on an expanded definition. When particular groups are targeted by censorship technologies, there are effects on affective life (individual identities, including gender and ethnic identifications) and communal areas of value (social relationships and, at the larger scale, national identities). It is possible that digital censorship could decrease such nonphysical violence in cases where older forms of technology (films, books, television) are less controlled due to a focus on social media communications; however, there is little empirical evidence for this. An expanded definition of violence highlights the severity of harms caused by complementary uses of OCCs, especially in repressive situations.

## Conclusion

States are a significant—although far from the only—source of violence in international politics. The development of new violent capacities, in the form of OCCs, poses important questions at both theoretical and policy levels. Theoretically, the increasingly prevalent harmful use of OCCs under the threshold of armed conflict challenges conventional understandings of their nonviolent nature in cyber conflict studies. It also calls for a deeper dialogue with other parts of the discipline that has considered repertoires and logics of violence in more detail, especially the study of political violence. Writing of this research area, DeMerritt suggests that "empirical regularities about how governments set the severity of repression and how they select from the set of available repressive tactics have not yet crystallized" (DeMerritt 2016, 6). If the selection process between differently violent (or "severe") options has not crystallized for repressive tactics in general, it is positively murky for OCCs, in both repressive and interstate contexts.

This article has argued that the strategic integration of OCOs into violent state capacities can be fruitfully analyzed through three logics: substitution, support, and complement. Our brief overview of the public record on OCOs has sought to demonstrate the plausibility of this argument. The article also illustrates why it is important to consider interstate and repressive contexts together. One of the features of new technologies, like OCCs, is learning and overlap between different forms and sites of violence: interstate violence easily shifts to repression while repressive tactics can be used externally as foreign interference.

As cyber capabilities mature, we anticipate that they will be used more frequently. Consequently, we expect

state learning and evolution of strategic thinking on cyber capabilities to affect these three logics in the future. OCCs are likely to act more as substitutes in those areas where they become more precise and effects more deterministic. Supportive logics will be more prevalent overall, as an increasing digitization of societies worldwide renders cyber capabilities even more crucial in enabling conventional operations. Complementary uses will continue to be experimental, as in the case of NotPetya. We anticipate such complementary uses to grow and diversify until either a dominant strategy crystallizes or their effects become so large that they become intolerable to the international community, leading to agreement of nonuse.

At a policy level, concerns around escalation as a result of cyber operations should be reoriented toward *violent* escalation, recognizing that some uses of OCCs could be strategically escalatory—raising the level of consequences for cyber operations, as with the recent SolarWinds compromise (Lubin 2020)—but without an accompanying increase in violence. Policy responses to cyber operations should be calibrated based on their logics of integration: supportive and substitutive uses are more likely to be amenable to existing frameworks, while complementary uses present a far more novel policy challenge. Acknowledging complementary uses of OCCs and understanding their violent effects gives defenders a better grasp of the complexity of defending against adversarial actions across a mostly civilian cyberspace.

Further research is required to systematically investigate the three logics of integration identified in this article in more detail. Such research should analyze cyber operations within their strategic context, rather than as standalone actions "in cyberspace." More specifically, data collection on OCOs should include the spectrum of alternative, non-cyber, options. In order to incorporate "negative" cases into databases on cyber operations, analysts should be alert for evidence of cyber options that are available but not used.

Finally, in addition to more extensive empirical testing and data-gathering, further research on logics of integration should move beyond the statist frame adopted in this article, in two ways. First, it should recognize that states are not unitary actors and have developed sophisticated practices for collectively committing violent acts. Such research would explore how OCCs create new forms of bureaucratic politics, generating opportunities and areas of friction within the organizational structure of the state, especially those elements that operate other violent capabilities: militaries, intelligence agencies, and police and security forces (Koren and Mukherjee 2020). Second, it should explore the political economy of OCCs in relation to their logics of integration, especially the role of private companies in building, supplying, and maintaining OCCs.

In this way, the framework of the three logics of integration presented in this article not only represents an important advance in bringing together scholarship on political violence and cyber conflict, but also provides a productive research agenda for the future.

## Acknowledgments

We thank our colleagues, the editors, and three anonymous reviewers for their constructive feedback and suggestions. Earlier versions of this article were presented at the International Studies Association (ISA) conference in Toronto in March 2019, the Center for Security Studies (CSS) research colloquium in July 2019, the Leiden Institute of Security and Global Affairs (ISGA) research seminar in November 2019, and the Digital Democracy Workshop organized by the Digital Democracy Lab at University of Zurich in November 2020. We thank all participants for their helpful feedback.

## References

Adee, Sally. 2008. "The Hunt for the Kill Switch: IEEE Spectrum." *IEEE Spectrum: Technology, Engineering, and Science News*, May 1, 2008. Accessed October 21, 2021. https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

Ali, Idrees, and Phil Stewart. 2019. "Exclusive: U.S. Carried out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials." *Reuters*, October 16, 2019. Accessed October 21, 2021. https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK.

Allen, Susan Hannah, and Carla Martinez Machain. 2018. "Choosing Air Strikes." *Journal of Global Security Studies* 3 (2): 150–62.

Al-Rawi, Ahmed K. 2014. "Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army." *Public Relations Review* 40 (3): 420–28.

Asal, Victor, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins, and Chris Bronk. 2016. "Repression, Education, and Politically Motivated Cyberattacks." *Journal of Global Security Studies* 1 (3): 235–47.

Baezner, Marie. 2017. "The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict." CSS Cyber Defense Project. Center for Security Studies, ETH Zurich.

Barnes, Julian E. 2018. "C.I.A. Concludes That Saudi Crown Prince Ordered Khashoggi Killed." *The New York Times*, November 17, 2018. Accessed October 21, 2021. https://perma.cc/KG6E-UNYA.

Baron, Ilan Zvi, Jonathan Havercroft, Isaac Kamola, Jonneke Koomen, Justin Murphy, and Alex Prichard. 2019. "Liberal Pacification and the Phenomenology of Violence." *International Studies Quarterly* 63 (1): 199–212.

Barrett, Edward. 2017. "On the Relationship Between the Ethics and the Law of War: Cyber Operations and Sublethal Harm." *Ethics & International Affairs* 31 (4): 467–77.

Bergman, Ronen, and Mark Mazzetti. 2019. "The Secret History of the Push to Strike Iran." *The New York Times*, September 4, 2019. Accessed October 21, 2021. https://perma.cc/4JL6-4H7L.

Betz, David J., and Tim Stevens. 2013. "Analogical Reasoning and Cyber Security." *Security Dialogue* 44 (2): 147–64.

Bolton, John. 2020. *The Room Where It Happened: A White House Memoir*. New York: Simon & Schuster.

Borghard, Erica D., and Shawn W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 452–81.

———. 2016. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*, 1st ed. Athens, GA: University of Georgia Press.

Brantly, Aaron F. 2017. "The Violence of Hacking: State Violence and Cyberspace." *The Cyber Defense Review* 2 (1): 73–92.

Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press.

Bufacchi, Vittorio. 2005. "Two Concepts of Violence." *Political Studies Review* 3 (2): 193–204.

Burgess, Mike. 2019. "Director-General ASD Speech to the Lowy Institute." *Australian Signals Directorate (ASD)*, March 27, 2019. Accessed October 21, 2021. https://perma.cc/VVM3-GZHX.

Clark, David H., and William Reed. 2005. "The Strategic Sources of Foreign Policy Substitution." *American Journal of Political Science* 49 (3): 609–24.

Cohn, Carol. 1987. "Sex and Death in the Rational World of Defense Intellectuals." *Signs: Journal of Women in Culture and Society* 12 (4): 687–718.

Council on Foreign Relations nd. "Cyber Operations Tracker." Accessed October 21, 2021. https://www.cfr.org/cyber-operations/.

Dalek, Jakub, Masashi Crete-Nishihata, and John Scott-Railton. "Shifting Tactics: Tracking Changes in Years-Long Espionage Campaign against Tibetans." *The Citizen Lab*, March 10, 2016.

Davenport, Christian. 2007. "State Repression and Political Order." *Annual Review of Political Science* 10 (1): 1–23.

Davenport, Christian, and Molly Inman. 2012. "The State of State Repression Research since the 1990s." *Terrorism and Political Violence* 24 (4): 619–34.

Deibert, Ronald J. 2020. *Reset: Reclaiming the Internet for Civil Society*. Canada: House of Anansi Press Ltd.

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. 2012. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." *Security Dialogue* 43 (1): 3–24.

DeMerritt, Jacqueline H.R. 2016. "The Strategic Use of State Repression and Political Violence." *Oxford Research Encyclopedia of Politics*, October.

Denning, Dorothy. 2012. "Stuxnet: What Has Changed?" *Future Internet* 4 (3): 672–87.

Dunn Cavelty, Myriam. 2008. *Cyber-Security and Threat Politics*. London: Routledge.

———. 2013. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15 (1): 105–22.

Durante, Massimo. 2015. "Violence, Just Cyber War and Information." *Philosophy & Technology* 28 (3): 369–85.

Dvilyanski, Mike, and Nathaniel Gleicher. "Taking Action against Hackers in China." *About Facebook (blog)*, March 24, 2021. Accessed October 21, 2021. https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/.

Egloff, Florian J. 2020a. "Contested Public Attributions of Cyber Incidents and the Role of Academia." *Contemporary Security Policy* 41 (1): 55–81.

———. 2020b. "Public Attribution of Cyber Intrusions." *Journal of Cybersecurity* 6 (1): 1–12.

———. 2021. "Intentions and Cyberterrorism." In: *Oxford Handbook of Cyber Security*, edited by Cornish, Paul. Oxford: Oxford University Press: 187–200.

Egloff, Florian J., and James Shires. 2021. "The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence." *European Journal of International Security*, online preprint 12 October 2021: 1–20. doi:10.1017/eis.2021.20.

Egloff, Florian J., and Max W. Smeets. 2021. "Publicly Attributing Cyber Attacks: A Framework." *Journal of Strategic Studies*, online preprint 10 March 2021: 1–32.

Farrell, Henry, and Charles L. Glaser. 2017. "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine." *Journal of Cybersecurity* 3 (1): 7–17.

FBI Records. nd. "COINTELPRO." *Folder. The Vault*. Accessed January 15, 2021. Accessed October 21, 2021. https://vault.fbi.gov/cointel-pro.

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organization* 49 (3): 379–414.

Fidler, David P. 2016. "Just & Unjust War, Uses of Force & Coercion: An Ethical Inquiry with Cyber Illustrations." *Daedalus* 145 (4): 37–49.

Finlay, Christopher J. 2018. "Just War, Cyber War, and the Concept of Violence." *Philosophy & Technology* 31 (3): 357–77.

FireEye Intelligence. 2018. "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers." *FireEye*. October 23, 2018. Accessed October 21, 2021. https://perma.cc/V2CV-UG7S.

Frazer, Elizabeth, and Kimberly Hutchings. 2008. "On Politics and Violence: Arendt Contra Fanon." *Contemporary Political Theory* 7 (1): 90–108.

Futter, Andrew. 2018. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Washington, DC: Georgetown University Press.

Gaouette, Nicole, Jennifer Hansler, Pamela Brown, and Kevin Liptak. 2019. "Pompeo Says Saudi Attack an 'act of War' as Trump Sounds More Cautious Note." *CNN*. September 19, 2019. Accessed October 21, 2021. https://perma.cc/2LZ3-QR3L.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73.

Gartzke, Erik, and Jon R. Lindsay. 2017. "Thermonuclear Cyberwar." *Journal of Cybersecurity* 3 (1): 37–48.

———. 2018. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In *Coercion: The Power to Hurt in International Politics*, edited byGreenhill, Kelly M., and Peter Krause, 179–203. New York: Oxford University Press.

———, eds. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York: Oxford University Press.

Gioe, David V., Michael S. Goodman, and Tim Stevens. 2020. "Intelligence in the Cyber Era: Evolution or Revolution?" *Political Science Quarterly* 135 (2): 191–224.

Goddard, Stacie E., Paul K. MacDonald, and Daniel H. Nexon. 2019. "Repertoires of Statecraft: Instruments and Logics of Power Politics." *International Relations* 33 (2): 304–21.

Gohdes, Anita R. 2020. "Repression Technology: Internet Accessibility and State Violence." *American Journal of Political Science* 64 (3): 488–503.

Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday.

Gregory, Thomas 2015. "Drones, Targeted Killings, and the Limitations of International Law." *International Political Sociology* 9 (3): 197–212.

Gutiérrez-Sanín, Francisco, and Elisabeth Jean Wood. 2017. "What Should We Mean by 'Pattern of Political Violence'? Repertoire, Targeting, Frequency, and Technique." *Perspectives on Politics* 15 (1): 20–41.

Hall, Todd H., and Andrew A.G. Ross. 2015. "Affective Politics after 9/11." *International Organization* 69 (4): 847–79.

Haraway, Donna J. 1985. "Cyborg Manifesto: Science, Technology, and Social-Feminist in the Late 20th Century." *Social Review* 80: 65–108.

Harel, Amos, and Aluf Benn. 2018. "No Longer a Secret: How Israel Destroyed Syria's Nuclear Reactor." *Haaretz*, March 23, 2018. Accessed October 21, 2021. https://perma.cc/6RME-RK7A.

Harknett, Richard J., and Joseph S. Nye. 2017. "Is Deterrence Possible in Cyberspace?" *International Security* 42 (2): 196–99.

Harknett, Richard J., and Max Smeets. 2020. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies* March 1–34.

Harvey, David. 2005. *The New Imperialism*. Oxford: Oxford University Press.

Hassib, Bassant, and Shires, James. 2021. "Manipulating Uncertainty: Cybersecurity Politics in Egypt." *Journal of Cybersecurity* 7 (1): 1–16.

Healey, Jason. 2016. "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers." *SIPA Columbia Journal of International Affairs*, November 2016). Accessed October 21, 2021. https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process.

Healey, Jason, Neil Jenkins, and J.D. Work. 2020. "Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations." In *20/20 Vision: The Next Decade*. edited byJančárková, T., L. Lindström, M. Signoretti, I. Tolga, and G. Visky, 251–74. Tallinn: CCD COE Publications.

Hopf, Ted. 2010. "The Logic of Habit in International Relations." *European Journal of International Relations* 16 (4): 539–61.

International Committee of the Red Cross. 2019. "International Humanitarian Law and Cyber Operations during Armed Conflicts." Position Paper. ICRC, Geneva.

Kalyvas, Stathis N. 2019. "The Landscape of Political Violence." In *The Oxford Handbook of Terrorism*, edited byChenoweth, Erica, Richard English, Andreas Gofas, and Stathis N. Kalyvas, 11–33. New York: Oxford University Press.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.

Khoury, Jack. 2018. "Syria Blames Missiles, False Alarm on 'Joint Electronic Attack' by Israel and U.S." *Haaretz*, April 17, 2018. Accessed October 21, 2021. https://perma.cc/8YQK-RATT.

Kirchgaessner, Stephanie. "Exclusive: Saudi Dissident Warned by Canadian Police He is a Target." *The Guardian*, June 21, 2020. Accessed October 21, 2021. https://perma.cc/HDY3-44YA.

Koren, Ore, and Bumba Mukherjee. 2020. "Civil Dissent and Repression: An Agency-Centric Perspective." *Journal of Global Security Studies* 6 (3): ogaa051.

Krause, Keith. 2009. "Beyond Definition: Violence in a Global Perspective." *Global Crime* 10 (4): 337–55.

Kreps, Sarah, and Jacquelyn Schneider. 2019. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics." *Journal of Cybersecurity* 5 (1): tyz007.

Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10 (1): 86–103.

Leyen, Ursula von der. 2015. "Strategische Leitlinie Cyber-Verteidigung Im Geschäftsbereich BMVg." *Netzpolitik*, April 16, 2015. Accessed October 21, 2021. https://perma.cc/9T7A-DCPN.

Libicki, Martin C. 2012. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corporation.

Lindsay, Jon Randall. 2017. "Restrained by Design: The Political Economy of Cybersecurity." *Digital Policy, Regulation and Governance* 19 (6): 493–514.

Lubin, Asif. 2020. "SolarWinds as a Constitutive Moment: A New Agenda for International Law of Intelligence." *Just Security*, December 23, 2020. Accessed October 21, 2021. https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/.

Lupovici, Amir. 2016. "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives* 17 (3): 322–42.

Lyon, David. 2018. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge, MA: Polity Press.

MacAskill, Ewen. 2017. "HMS Queen Elizabeth Could Be Vulnerable to Cyber-Attack." *The Guardian*, June 26, 2017, sec. Technology. Accessed October 21, 2021. https://www.theguardian.com/technology/2017/jun/27/hms-queen-elizabeth-royal-navy-vulnerable-cyber-attack.

March, James G., and Johan P. Olsen. 1998. "The Institutional Dynamics of International Political Orders." *International Organization* 52 (4): 943–69.

Markoff, John, and Thom Shanker. 2009. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *The New York Times*, August 1, 2009, sec. U.S. Accessed October 21, 2021. https://perma.cc/4CFG-6DYG.

Martelle, Michael. 2020. "USCYBERCOM after Action Assessments of Operation GLOWING SYMPHONY." *Briefing Book 693*. Washington, DC: GWU National Security Archive.

Michaelsen, Marcus. 2017. "Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran." *Surveillance & Society* 15 (3/4): 465–70.

Moss, Dana M. 2018. "The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora." *Globalizations* 15 (2): 265–82.

Mozur, Paul, and Nicole Perlroth. 2020. "China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn." *The New York Times*, July 1, 2020, sec. Technology. Accessed October 21, 2021. https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html.

Nakashima, Ellen. 2019. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *Washington Post*, February 27, 2019. Accessed October 21, 2021. https://perma.cc/2VUB-CWPG.

Nye, Joseph S. 2011a. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5 (4): 18–38.

———. 2011b. *The Future of Power*. New York: PublicAffairs.

Öztürk, A. Erdi, and Hakki Taş. 2020. "The Repertoire of Extraterritorial Repression: Diasporas and Home States." *Migration Letters* 17 (1): 59–69.

Peterson, Dale. 2013. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* 36 (1): 120–24.

Pouliot, Vincent. 2008. "The Logic of Practicality: A Theory of Practice of Security Communities." *International Organization* 62 (2): 257–88.

Radu, Roxana. (2019). *Negotiating Internet Governance*. Oxford: Oxford University Press.

Ralston, William. 2020. "The Untold Story of a Cyberattack, a Hospital and a Dying Woman." *Wired UK*, November 11, 2020. Accessed October 21, 2021. https://www.wired.co.uk/article/ransomware-hospital-death-germany.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32.

———. 2013a. "More Attacks, Less Violence." *Journal of Strategic Studies* 36 (1): 139–42.

———. 2013b. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

———. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Profile Books.

Ritter, Emily Hencken, and Courtenay R. Conrad. 2016. "Preventing and Responding to Dissent: The Observational Challenges of Explaining Strategic Repression." *American Political Science Review* 110 (1): 85–99.

Roth, Florian. 2018. "The Newcomer's Guide to Cyber Threat Actor Naming." *Medium*, March 25, 2018. Accessed October 21, 2021. https://perma.cc/USH2-NESK.

Sanger, David E. 2013. *Confront and Conceal*. New York: Penguin Random House.

Schinkel, Willem. 2010. *Aspects of Violence*. Basingstoke: Palgrave Macmillan.

Schmitt, Eric, and Thom Shanker. 2011. "U.S. Debated Cyberwarfare in Attack Plan on Libya." *The New York Times*, October 17, 2011. Accessed October 21, 2021. https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schulzke, Marcusv. 2018. "The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty." *Perspectives on Politics* 16 (4): 954–68.

Scott, James C. 1999. *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, CT: Yale University Press.

Scott-Railton, John, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola. "Group5: Syria and the Iranian Connection." *Citizen Lab*, August 2, 2016.

Shepherd, Laura. 2013. *Gender, Violence and Security: Discourse as Practice*. London: Zed Books Ltd.

Shires, James. 2019. "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." *Journal of Cyber Policy* 4 (2): 235–56.

———. 2020. "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics." *Texas National Security Review* 3 (4): 10–29.

Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41 (3): 72–109.

———. 2021. "What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018." *Texas National Security Review* 4 (1): 62–96.

Smeets, Max. 2018a. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* 12: 90–113.

———. 2018b. "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment." *Defence Studies* 18 (4): 395–410.

Smeets, Max, and Robert Chesney. 2020. "Policy Roundtable: Cyber Conflict as an Intelligence Contest." *Texas National Security Review*, September 17, 2020. Accessed October 21, 2021. http://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

Smeets, Max, and Herbert Lin. 2018. "Offensive Cyber Capabilities: To What Ends?" In *CyCon X: Maximising Effects*. Tallinn: NATO CCD COE Publications.

Soliman, Mohammed. 2020. "The Rise of Digital Authoritarianism in the Middle East." In *Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, edited bySexton, Michael, and Eliza Campbell, 124–44. Washington, DC: Middle East Institute.

Stevens, Tim. 2015. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

———. 2017. "Cyberweapons: An Emerging Global Governance Architecture." *Palgrave Communications* 3 (16102).

Suchman, L, K. Follis, and J. Weber. 2017. "Tracking and Targeting: Sociotechnologies of (In)security." *Science, Technology, & Human Values* 42 (6): 983–1002.

Taillat, Stéphane. 2019. "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security." *Contemporary Security Policy* 40 (3): 368–81.

Thomas, Claire. 2011. "Why Don't We Talk about 'Violence' in International Relations?" *Review of International Studies* 37 (4): 1815–36.

UK National Audit Office. 2018. "Investigation: WannaCry Cyber Attack and the NHS." Report, April 25.

Valeriano, Brandon, and Benjamin Jensen. 2019. "How Cyber Operations Can Help Manage Crisis Escalation with Iran." *Washington Post*, June 25, 2019. Accessed October 21, 2021. https://perma.cc/8C8R-ASJL.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.

Valeriano, Brandon, Ryan C. Maness, and Benjamin Jensen. 2017. "Cyberwarfare Has Taken a New Turn. Yes, It's Time to Worry." *Washington Post*, July 13, 2017. Accessed October 21, 2021. https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/.

van Wagtendonk, Anya. 2019. "Trump Called off a Military Strike against Iran. The US Targeted Its Computer Systems Instead." *Vox*, June 23, 2019. Accessed October 21, 2021. https://perma.cc/UW9A-23BS.

White House. 2018. "Statement from the Press Secretary." *U.S. White House*. Accessed October 21, 2021. https://web.archive.org/web/20200526092648/https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

Whyte, Christopher. 2020. "Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online." *European Journal of International Security* 5 (2): 195–214.

Wilcox, Lauren B. 2015. *Bodies of Violence: Theorizing Embodied Subjects in International Relations*. 1st ed. Oxford: Oxford University Press.

Woodlock, Delanie. 2017. "The Abuse of Technology in Domestic Violence and Stalking." *Violence Against Women* 23 (5): 584–602.

Woodlock, Delanie, Mandy McKenzie, Deborah Western, and Bridget Harris. 2020. "Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control." *Australian Social Work* 73 (3): 368–80.

Work, J.D. 2019. "Calculating the Fast Equations: Arsenal Management Considerations in Sustained Offensive Cyber Operations." Presented at the Cyber Project Seminar, Belfer Center for Science and International Affairs, April 8. Accessed October 21, 2021. https://www.belfercenter.org/event/calculating-fast-equations-arsenal-management-considerations-sustained-offensive-cyber.

Zetter, Kim. 2014. *Countdown to Zero Day*. New York: Penguin Random House.