The better angels of our digital nature? Offensive cyber capabilities and state violence

Egloff, F.J.; Shires, J.

European Journal of International Security (2021), page 1 of 20
doi:10.1017/eis.2021.20

EJIS

RESEARCH ARTICLE

The better angels of our digital nature? Offensive cyber capabilities and state violence

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

[1]Center for Security Studies (CSS), ETH Zürich, Zürich, Switzerland and Centre for Technology and Global Affairs, Department of Politics; International Relations, University of Oxford, Oxford, United Kingdom and [2]Institute for Security and Global Affairs, Leiden University, The Hague, Netherlands; Cyber Statecraft Initiative, Atlantic Council, Washington, DC, United States
*Corresponding author. Email: florianegloff@ethz.ch

(Received 7 August 2020; revised 13 May 2021; accepted 18 August 2021)

Abstract

Transformations in state violence are intimately associated with technological capacity. Like previous era-defining technologies, global digital networks have changed state violence. Offensive cyber capabilities (OCCs) appear to constitute a major technological development that offers the potential for reducing state violence. This article asks: are OCCs really the better angels of our digital nature? Current scholarship in strategic studies, adopting a narrow definition of violence, conceives of OCCs as largely non-violent. This ignores how technology has given rise to new forms of harm to individuals and communities, particularly in the context of violent state repression. We propose using an expanded definition of violence, including affective and community harms, and argue that OCCs relocate, rather than reduce, state violence towards non-bodily harms. Even though their lethal effects are limited, OCCs are not, as is supposed, a non-violent addition to state arsenals. This conclusion has important implications for international affairs, including re-orienting defensive cybersecurity efforts and altering calculations around the perception of OCCs by adversaries.

Keywords: Cyber Security; Violence; International Security; International Relations Theory; Armed Conflict; Repression

Introduction

State violence has changed radically since the emergence of states in their modern form. These changes in violent action are bound up with – both cause and effect of – the transformation of the state itself over that time.[1] Transformations in state violence are also intimately associated with technological capacity.[2] States now have far greater ability to inflict violence than they

[1]Charles Tilly, *Coercion, Capital and European States, A.D. 990–1992* (Cambridge, MA: Wiley-Blackwell, 1992); James C. Scott, *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven, CT: Yale University Press, 1999); for a recent contribution, see Michael Mousseau, 'The end of war: How a robust marketplace and liberal hegemony are leading to perpetual world peace', *International Security*, 44:1 (2019), pp. 160–96, available at: {https://doi.org/10.1162/isec_a_00352}.

[2]See, for example, Geoffrey L. Herrera, *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change* (Albany, NY: State University of New York Press, 2007); Priya Satia, *Empire of Guns: The Violent Making of the Industrial Revolution* (Richmond, VA: Duckworth, 2019). As scholars in science and technology studies (STS) have long argued, this association is complex, with new forms of state violence appearing due to intricate interplays between individual innovations, scientific breakthroughs, technological inventions, strategic paradigm shifts, and broader cultural waves.

have ever previously possessed, but they have not – fortunately – deployed all their violent potential.[3]

Digital networks, including the Internet, are an era-defining set of communications technologies.[4] In addition to their social and economic benefits, digital networks subject individuals, organisations, and states to new and unpredictable risks. States are not always the masters of internet communications or infrastructure in their territory, and, as a corollary, they have a far greater reach than before into the territory of other states.[5]

The element of the digital revolution that has most clearly affected state violence is a set of technologies often referred to simply as 'cyberweapons', but more precisely as offensive cyber capabilities (OCCs). Academic scholarship has argued that OCCs are less violent *as a class of technologies* overall; in US terminology, as an entirely new – and strategically equivalent – 'domain' of warfare.[6] This is so despite the prevalence of 'cyber-bombs', a 'digital Pearl Harbor', and other disaster scenarios that appear regularly in both the popular and professional imagination. OCCs thus seem to fit into the civilising logic identified by Norbert Elias and popularised by psychologist Steven Pinker in his well-known book tracking trends in human violence for millennia.[7] In Pinkerian terms, offensive cyber capabilities may be the better angels of our digital nature, because they are an addition to the coercive repertoires of states that is less violent than the alternatives.

This article assesses this proposition and thus contributes to scholarship on cyber conflict and International Relations. It shows how the strategic studies and International Relations literature on OCCs conceives them as non-violent by adopting a narrow definition of violence as lethal bodily harm. It then argues that this narrow definition of violence inadequately captures key analytical distinctions between the range of supposedly 'non-violent' harms associated with OCCs, especially in repressive contexts. Consequently, the concept of violence should be expanded to accommodate relevant violations that occur using OCCs. In short, OCCs relocate, rather than reduce, state violence.

More is at stake than analytical leverage. Expanding the concept of violence in relation to OCCs closely tracks current policy interventions that pursue the normative goal of reducing the level of cyber-related harms in international politics.[8] The dominance of a narrow conception of violence means that many states have used OCCs to undertake significant harmful actions in their own and each other's societies without recognising the extent of such harms. An expanded concept of violence as intentional proximate harm to areas of human value – including the body, affective life,

[3]The comprehensive study of deterrence and nuclear logics during the Cold War was primarily an effort to understand why and how such restraint is possible. For a recent discussion of a vast literature, see Keir A. Lieber and Daryl G. Press, 'The new era of counterforce: Technological change and the future of nuclear deterrence', *International Security*, 41:4 (2017), pp. 9–49, available at: {https://doi.org/10.1162/ISEC_a_00273}.

[4]Early insights into characteristics of the digital era can be found in Manuel Castells, *Rise of the Network Society, Vol. 1* (Malden, MA: Wiley-Blackwell, 1996); Ronald J. Deibert, *Parchment, Printing and Hypermedia: Communication and World Order Transformation* (New York, NY: Columbia University Press, 1997); James N. Rosenau and J. P. Singh (eds), *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (Albany, NY: State University of New York Press, 2002).

[5]On the Internet and territory, see Didier Bigo, Engin Isin, and Evelyn Ruppert (eds), *Data Politics: Worlds, Subjects, Rights* (London, UK and New York, NY: Routledge, 2019), especially the chapter by Deibert and Pauly; also Daniel Lambach, 'The territorialization of cyberspace', *International Studies Review* (2019), available at: {https://doi.org/10.1093/isr/viz022}.

[6]This terminology emerged along with the creation of the US Cyber Command in 2009–10. For an influential statement, see William J. Lynn III, 'Defending a new domain', *Foreign Affairs* (2010), available at: {https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain}.

[7]Norbert Elias, *The Civilizing Process: Sociogenetic and Psychogenetic Investigations* (rev. edn, Oxford, UK and Malden, MA: Blackwell Publishing, 2000 [orig. pub. 1936]); Stephen Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York, NY: Penguin Group USA, 2015).

[8]For example, see the recent statement by Nils Melzer, the UN Special Rapporteur on torture. Owen Bowcott, 'UN warns of rise of "cybertorture" to bypass physical ban', *The Guardian* (21 February 2020), available at: {https://www.theguardian.com/law/2020/feb/21/un-rapporteur-warns-of-rise-of-cybertorture-to-bypass-physical-ban}.

and social relationships – not only provides greater analytical traction than broader notions of harm in understanding the impact of OCCs, but, by mobilising the normative weight of the concept of violence, also justifies a policy focus on countering and ameliorating those harms.

The intervention of this article – the expanded concept of violence – is theoretical. The aim is not to test the violence of OCCs systematically, but to provide a reconceptualisation that can capture relevant harms occurring in cyberspace. Further research should investigate this in more detail, using large-n and detailed qualitative methods to explore OCCs' violent effects through long-term trends and in specific cases.

The article is structured in six parts. The first part defines OCCs. The second part introduces the existing strategic studies literature on OCCs, dominated by a narrow conception of violence as physical or lethal harm. The third part then explores the concept of violence in more depth, drawing on scholarship across philosophy and the social sciences. The fourth part applies this expanded conception of violence to OCCs, showing how it offers new ways of understanding harms occurring from both interstate and repressive uses of OCCs. The fifth part considers the risks of conceptual expansion, and the sixth part concludes by returning to the policy imperative introduced above.

What are offensive cyber capabilities?

OCCs are the combination of various elements that jointly enable the adversarial manipulation of digital services or networks.[9] 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 organisational capacity to perform 'arsenal management' and obtain bureaucratic and legal authorities for action.[10] Thus, the broad term OCCs includes what others see as cyber 'weapons' (that is, artifacts that can cause harm), in the sense of a sitting arsenal, but in addition highlights the organisational, technological, and human investment brought to bear in an ad-hoc and highly tailored manner for specific missions.[11] A prominent historical example of OCCs would be the ability to covertly manipulate the programmable logic controllers at the nuclear enrichment facility in Natanz (Iran) to degrade the enrichment centrifuges, often referred to by the name given to the worm implementing that effect, Stuxnet, but more aptly captured by the operation name given to the development and deployment of the capability, Olympic Games.[12] This operation was first discovered publicly in 2010 but with earlier versions operational several years earlier.[13]

In the terminology of the United States Air Force, adversarial manipulation aims to disrupt, degrade, or destroy the targeted network or connected systems, or to deceive or deny adversaries

[9]Dale Peterson, 'Offensive cyber weapons: Construction, development, and employment', *Journal of Strategic Studies*, 36:1 (2013), pp. 120–4, available at: {https://doi.org/10.1080/01402390.2012.742014}. 'Adversarial' simply means against the target's interests.

[10]Jason Healey, 'The U.S. government and zero-day vulnerabilities: From pre-heartbleed to shadow brokers', *SIPA Columbia Journal of International Affairs* (2016); Rebecca Slayton, 'What is the cyber offense-defense balance? Conceptions, causes, and assessment', *International Security*, 41:3 (1 January 2017), pp. 72–109; J. D. Work, 'Calculating the Fast Equations: Arsenal Management Considerations in Sustained Offensive Cyber Operations', Cyber Project Seminar, Belfer Center for Science and International Affairs (8 April 2019).

[11]Conventional weapons also rely on expertise, maintenance, and intelligence infrastructure, but the increased speed with which cyberspace changes in relation to physical space means that conventional weapons last for longer. Max Smeets, 'A matter of time: On the transitory nature of cyberweapons', *Journal of Strategic Studies*, 42:1–2 (2017), pp. 1–28. See also Slayton, 'What is the cyber offense-defense balance?'.

[12]Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (1st edn, New York, NY: Crown Publishers, 2014); for a detailed exploration of the organisational challenges involved in building that capability, see Rebecca Slayton, 'What is the cyber offense-defense balance? Conceptions, causes, and assessment', *International Security*, 41:3 (2017), pp. 72–109.

[13]Ralph Langner, 'To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve', The Langner Group (November 2013); Kim Zetter, *Countdown to Zero Day* (New York, NY: Penguin Random House, 2014).

access to that network or connected systems (the 5 Ds).[14] OCCs generally require some level of unauthorised access, unless their aim is only to 'deny' access to online services. They also usually involve external control of the network over the Internet, but this is not always the case: the Stuxnet malware was manually inserted into an 'air-gapped' industrial control network.[15] In addition to the 5 Ds, OCCs can also enable 'exfiltration' – the copying of data from the target network – because the same exploitation techniques are used prior to the 'payload' stage. Consequently, cyber espionage and preparation for disruption can (but do not have to) look identical from the victim's perspective, with sophisticated technical analysis and wider threat characteristics required to distinguish between the two.[16]

Many states have developed and used OCCs in the last decade, including the United States and its allies, and we briefly review some key incidents, operations, and campaigns in the following paragraphs.[17] It should be noted that offensive cyber capabilities are often used by private actors on behalf of states, or by proxies.[18]

In addition to the Stuxnet operation, the US also created a plan to use OCCs to disable Iranian networks nationwide in order to degrade and deny them to Iran in case of conflict (Operation NITRO ZEUS), developed under the current head of US Cyber Command, Gen. Paul Nakasone.[19] Another notable Israel-attributed virus discovered in 2011, Duqu, was also aimed at industrial control systems.[20] The Snowden disclosures in 2013 revealed cyber operations by the Five Eyes intelligence partners (US, UK, Canada, Australia, New Zealand), including 'effects' operations and offensive cyber operations enabling signals intelligence collection by UK's GCHQ.[21] Other US and allied cyber operations to collect intelligence and to deceive ISIS leadership were mounted against ISIS in Syria.[22] More recently, in both June and September 2019, the US claimed to have conducted cyber operations against Iran in retaliation to the downing of an unmanned US surveillance drone and attacks against oil facilities in Saudi Arabia.[23]

[14]Deborah Bodeau and Richard Graubert, 'Characterizing Effects on the Cyber Adversary' (Bedford, MA: The MITRE Corporation, November 2013); US Air Force, 'Department of Defense Fiscal Year (FY) 2014 President's Budget Submission', Research, Development, Test and Evaluation, Vol 1 (US Air Force, April 2013), p. 161.

[15]Kim Zetter and Huib Modderkolk, 'Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran', *Yahoo! News* (2 September 2019), available at: {https://perma.cc/3AB6-AX8T}.

[16]Buchanan uses this fact to argue that OCCs create an escalation risk. Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London, UK: Hurst, 2017).

[17]Smeets highlights unsubstantiated claims by US officials in 2018 that over one hundred states were capable of launching cyberattacks. Max Smeets, 'The strategic promise of offensive cyber operations', *Strategic Studies Quarterly* (2018), pp. 90–113; increasingly, impactful campaigns, including some of the ones discussed below, are publicly attributed by states; see Florian J. Egloff, 'Public attribution of cyber intrusions', *Journal of Cybersecurity*, 6:1 (2020), pp. 1–12, available at: {https://doi.org/10.1093/cybsec/tyaa012}; Florian J. Egloff and Max Smeets, 'Publicly attributing cyber attacks: A framework', *Journal of Strategic Studies* (2021), pp. 1–32, available at: {https://doi.org/10.1080/01402390.2021.1895117}.

[18]Florian J. Egloff, 'Cybersecurity and the age of privateering', in George Perkovich and Ariel Levite (eds), *Understanding Cyberconflict: Fourteen Analogies* (Washington, DC: Georgetown University Press, 2017), pp. 231–47; Lucas Kello, 'Private sector cyber weapons: An adequate response to the sovereignty gap?', in Herbert Lin and Amy Zegart (eds), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington, DC: Brookings Institution Press, 2019); Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, MA: Cambridge University Press, 2018).

[19]David E. Sanger and Mark Mazzetti, 'US had cyberattack plan if Iran nuclear dispute led to conflict', *The New York Times* (16 February 2016), available at: {https://perma.cc/ZS2Y-UCQZ}.

[20]Symantec, 'W32. Duqu: The Precursor to the Next Stuxnet' (23 November 2011).

[21]'JTRIG tools and techniques', *The Intercept* (14 July 2014), available at: {https://perma.cc/8ZEV-UB4Q}; Ryan Gallagher, 'The inside story of how British spies hacked Belgium's largest Telco', *The Intercept* (blog) (13 December 2014), available at: {https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/}.

[22]Michael Martelle, 'USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY' (Washington, DC: GWU National Security Archive, 21 January 2020), available at: {https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony}.

[23]Idrees Ali and Phil Stewart, 'Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: Officials', *Reuters* (16 October 2019), available at: {https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK}.

States with a more adversarial relationship with the US, such as Iran, Russia, China, and North Korea, have also developed OCCs. Notably, an Iran-attributed data deletion attack in August 2012 ('Shamoon') on Saudi Aramco and Qatari company RasGas, re-engineered elements of US/Israeli OCCs discovered in Iran, to wipe data on and render thirty thousand computers dysfunctional.[24] This was followed by distributed denial of service (DDoS) attacks on US banks in 2012 among other incidents.[25]

Some of the most serious incidents attributed to Russia to date include disruptive operations against Ukraine's electrical grid in 2015 and 2016 (Black/Grey Energy) and the NotPetya virus, which infected shipping company Maersk, among others, in 2017.[26] Subsequent OCCs attributed to Russian entities include a virus in Saudi petrochemical plants in 2017, which included a module that manipulated safety systems (Triton/Trisis).[27]

Although Chinese OCCs have been used primarily for espionage,[28] North Korea has used OCCs for disruption, with the Sony Pictures hack-and-leak in 2014 claimed by 'Guardians of Peace', a hacker group attributed to the North Korean government. Infiltrations into the payment system underpinning international financial transactions (SWIFT) and the Central Bank of Bangladesh in 2016, and the 'Wannacry' ransomware that spread worldwide in 2017, including a brief paralysis of the UK's National Health Service, have also been attributed to North Korea.[29]

However, despite the extensive deployment of OCCs by states, accompanied by a powerful narrative around cyber 'hype', OCCs have not caused destruction on a scale comparable to conventional weaponry. Despite extensive disruption from the incidents reviewed above, with significant economic losses, systems recovered shortly afterwards, albeit with intense effort, and no one died. This fact is the basis for a strand of academic thinking arguing that OCCs are less violent than other forms of military power, to which we now turn.

A narrow definition of violence

This section traces thinking on violence in key works on cybersecurity in International Relations and strategic studies. Although Thomas Rid's seminal article and book, 'Cyber War Will Not Take Place',[30] prompted a brief surge in debate on the concept of violence, the dominant strand of academic reasoning both before and after has been that OCCs are non-violent alternatives to conventional means, relying on a narrow concept of violence as lethal bodily harm. This section argues that such a narrow definition unhelpfully classes together a range of supposedly 'non-violent' harms associated with OCCs. Although scholars have frequently pointed to the importance of these harms, they nonetheless classify them equally as non-violent, missing an analytically useful distinction.

[24]Christopher Bronk and Eneken Tikk-Ringas, 'The cyber attack on Saudi Aramco', *Survival*, 55:2 (2013), pp. 81–96. Updated versions of the Shamoon virus returned in Saudi Arabia between 2016 and 2018, while Iran-attributed attacks on critical infrastructure in Bahrain were reported in July 2019.

[25]US Department of Justice, 'Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector' (Office of Public Affairs, 24 March 2016), available at: {https://perma.cc/S7YF-DZGP}. For further discussion on the regional impact of the incidents in this paragraph, see James Shires, *The Politics of Cybersecurity in the Middle East* (London, UK: Hurst, 2021), ch. 3.

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

[27]Blake Sobczak, 'The inside story of the world's most dangerous malware', *E&E News* (7 March 2019), available at: {https://perma.cc/H8R6-RY3A}.

[28]Andrea Gilli and Mauro Gilli, 'Why China has not caught up yet: Military-technological auperiority and the limits of imitation, reverse engineering, and cyber espionage', *International Security*, 43:3 (2019), pp. 141–89, available at: {https://doi.org/10.1162/isec_a_00337}.

[29]US Department of the Treasury, 'Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups' (13 September 2019), available at: {https://home.treasury.gov/index.php/news/press-releases/sm774}.

[30]Thomas Rid, 'Cyber war will not take place', *Journal of Strategic Studies*, 35:1 (2012), pp. 5–32; Thomas Rid, *Cyber War Will Not Take Place* (Oxford, UK and New York, NY: Oxford University Press, 2013).

It should be noted that many of these scholars do not include espionage activity in their definition of OCCs.[31] However, given the extensive overlap between cyber capabilities deployed for espionage and disruptive purposes, we do not exclude such activity by definition, and examine its relevance for violence in subsequent sections.

The violence – or lack thereof – of OCCs was a key concern for scholars of technology and war well before the emergence of the cyber lexicon itself. Early on in the development of thought on the military potential of digital technologies, and well before the commonplace use of OCCs, John Arquilla and David Ronfeldt declared that 'most netwars will probably be non-violent',[32] while Giampiero Giacomello expressed doubts that computer network operations were likely to 'break things and kill people (BTKP)'.[33] In the following decade, Ralf Bendrath concluded that 'in bodyless cyberspace there is no room for physical violence',[34] while Myriam Dunn Cavelty's investigation of US cyber policy argued that 'dropping the word "war" in dealing with information activities … stresses or implies [their] non-violent nature'.[35] There were dissenting voices even in these early debates: Martin Van Creveld suggested in 2002 that the 'greatest single shortcoming' of his 1989 magnum opus *The Transformation of War* had been to omit information warfare, which could 'lead to the deaths of millions' in cases where electricity grids were shut off or stock markets crashed.[36]

Following Stuxnet, such disaster scenarios abounded, provoking an extensive debate on their accuracy and questions of threat inflation and construction.[37] This literature followed securitisation scholarship in treating the question of violence tangentially, focusing more on the means by which threat representations gain prominence.[38] The strategic studies community, in contrast, focused directly on the *lack* of violence demonstrated by Stuxnet-type attacks. In 2011, Tim Maurer argued that 'cyberwarfare costs fewer lives compared with traditional types of warfare',[39] while Martin C. Libicki poured further cold water on the flames of cyber war, claiming that 'there is scant indication that a full-blown attack could kill as many as a normal year's flu epidemic'.[40] Dorothy Denning suggested that Stuxnet itself presented 'less harm and risk than the kinetic weapon'.[41] Although these scholars saw Stuxnet as merely *less* violent than conventional alternatives, others were more explicit in identifying violence with lethal bodily harm, as follows.

The question of violence was treated extensively in two influential exchanges: the first between Thomas Rid and John Stone, and the second between Erik Gartzke, Lucas Kello, and Jon R. Lindsay.[42] Rid approached OCCs through his examination of cyberwar. In doing so, he

[31]A view reflected in the discussions of the relevant UN Group of Governmental Experts (GGE), likely for political and legal convenience.

[32]John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington, DC: RAND Corporation, 1997), p. 29.

[33]Giampiero Giacomello, 'Measuring "digital wars": Learning from the experience of peace research and arms control', *Infocon Magazine* (October 2003), p. 8.

[34]Ralf Bendrath, 'The cyberwar debate: Perception and politics in US critical infrastructure protection', *Information & Security: An International Journal*, 7 (2001), pp. 80–103 (p. 92).

[35]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics* (London, UK and New York, NY: Routledge, 2008), p. 72.

[36]Martin Van Creveld, 'The transformation of war revisited', *Small Wars & Insurgencies*, 13:2 (2002), pp. pp. 9–10, available at: {https://doi.org/10.1080/09592310208559177}.

[37]Key contributions include Myriam Dunn Cavelty, 'From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse', *International Studies Review*, 15:1 (2013), pp. 105–22, available at: {https://doi.org/10.1111/misr.12023}; Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge, UK: Cambridge University Press, 2015), p. 103.

[38]Lene Hansen and Helen Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, 53:4 (2009), pp. 1155–75.

[39]Tim Maurer, 'The case for cyberwarfare', *Foreign Policy* (19 October 2011), available at: {https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/}.

[40]Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012), p. 77.

[41]Dorothy Denning, 'Stuxnet: What has changed?', *Future Internet*, 4 (2012), pp. 672–87 (p. 684).

[42]Rid, 'Cyber war will not take place' (2012); John Stone, 'Cyber war will take place!', *Journal of Strategic Studies*, 36:1 (2013), pp. 101–08; Erik Gartzke, 'The myth of cyberwar: Bringing war in cyberspace back down to Earth', *International*

employed a narrowly physical view of violence disassociated from harm or damage: for example, stating that 'non-violent cyber attacks *could* cause economic consequences without violent effects that *could* exceed the harm of an otherwise smaller physical attack'.[43] Stone's response argues that Rid's argument slips between violence and force, countering that 'all war involves force, but force does not necessarily imply violence – particularly if violence implies lethality'.[44] For Stone, OCCs are a 'violence multiplier' rather than a force multiplier, illustrated by analogies with bombing raids that cause only building damage and a stiletto that kills with almost no force. Nonetheless, Stone's view of violence remains physical, focused mainly on lethal harm. Rid's response in turn is even clearer: titled 'More Attacks, Less Violence', he concludes that 'the rise of cyber attacks *reduces* the amount of violence'.[45]

Kello's treatment of violence is more cautious than Rid's, as he describes OCCs as not being 'overtly violent' or distinguishes them from 'traditional violence', leaving room for covert or non-traditional violence.[46] However, Kello's work is symptomatic of a wider movement in the field from questions of violence to questions of effect, as he focuses not on violence but on 'potency'.[47] The concept of potency asks whether cyber weapons are efficacious or powerful, *not* whether they are violent.[48] More recent work by others along these lines also examines 'dangerous' instability rather than explicitly considering violence.[49]

This movement away from violence is most explicitly made by Gartzke, who suggests that Rid's definitional debate 'risks becoming a purely academic exercise' if cyberwar fulfils the same strategic logic as traditional war.[50] Gartzke focuses on the potential of 'the Internet to carry out functions commonly identified with terrestrial political violence', rather than the question of whether those functions would also be violent if carried out over the Internet.[51] He addresses conceptual issues of damage and harm only briefly, arguing that cyberwar is less effective because damage is temporary, and its use degrades capabilities, so it should remain adjunct to terrestrial force.[52] Following this debate, the concept of violence is now used rarely by strategic studies scholars

Security, 38:2 (2013), pp. 41–73; Lucas Kello, 'The meaning of the cyber revolution: Perils to theory and statecraft', *International Security*, 38:2 (2013), pp. 7–40; Jon R. Lindsay and Lucas Kello, 'Correspondence: A cyber disagreement', *International Security*, 39:2 (2014), pp. 181–92, available at: {https://doi.org/10.1162/ISEC_c_00169}.

[43]Rid, 'Cyber war will not take place' (2012), p. 9. Emphasis in original. Importantly, Rid's focus was on war, and violence was not his main concern. We discuss it here, as it led to one of the earlier disagreements in writing about violence through cyber means. In another place, Rid and McBurney did include mental harm as part of their 'weapon' definition; see Thomas Rid and Peter McBurney, 'Cyber-weapons', *The RUSI Journal*, 157:1 (2012), pp. 6–13, available at: {https//doi: 10.1080/03071847.2012.664354}.

[44]Stone, 'Cyber war will take place!', p. 103.

[45]Thomas Rid, 'More attacks, less violence', *Journal of Strategic Studies*, 36:1 (1 February 2013), pp. 139–42 (p. 142), available at: {https://doi.org/10.1080/01402390.2012.742012}. Violence here is clearly bodily: Rid states that because 'the human body, in several ways, is the foundation of violence' (p. 140), and 'computer code, on its own, cannot harm a biological system', then 'the human body is not directly vulnerable to cyber attack' (p. 139). We agree with Rid here but seek to expand the concept of violence beyond the body. We return to the concept of 'indirect' violence proposed in Rid's response in section 4 below.

[46]Elsewhere, Kello implies that cyber capabilities are entirely non-violent: 'machine functions have replaced violent charges in the behaviour of weapons'. Kello, *The Virtual Weapon and International Order*, p. 61. His views on this evolve: In 2013, Kello suggested that OCCs can cause 'direct injury to the victim', and in 2017 added that they cause 'direct injury to machines'. Kello, 'The meaning of the cyber revolution', p. 25; Kello, *The Virtual Weapon and International Order*, p. 65.

[47]See, for example, Lindsay and Kello, 'Correspondence', p. 189.

[48]See Henry Farrell and Charles L. Glaser, 'The role of effects, saliencies and norms in US cyberwar doctrine', *Journal of Cybersecurity*, 3:1 (2017), pp. 7–17, available at: {https://doi.org/10.1093/cybsec/tyw015}. Also Slayton's discussion of costs and benefits of OCCs in Slayton, 'What is the cyber offense-defense balance?'.

[49]Jacquelyn Schneider, 'The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war', *Journal of Strategic Studies*, 42:6 (2019), pp. 841–63, available at: {https://doi.org/10.1080/01402390.2019.1627209}.

[50]Gartzke, 'The myth of cyberwar', p. 49.

[51]Ibid., p. 42.

[52]Ibid., pp. 57–9.

focusing on cybersecurity, including those reviewed above, and given little theoretical attention.[53]

In sum, key works in the strategic studies literature on OCCs largely treat them as non-violent alternatives to conventional means, based on a narrow, physical (kinetic) and/or lethal definition of violence. This argument has been the basis for much of the subsequent research in the field focusing on specific strategic concepts, including deterrence[54] and coercion.[55] Indeed, a lack of physical violence is part of the reason for the strategic utility of OCCs highlighted by this literature.

At this stage, we can be more precise about the contribution of this article to the literature above. We do not claim that scholars such as Rid, Gartzke, and Kello above, or other influential analysts such as Adam P. Liff, Richard J. Harknett, and Max Smeets, overlook or are uninterested in the harmful effects of cyber operations, particularly below the threshold of armed conflict – they undoubtedly are.[56] Indeed, their work highlights these harms as strategically relevant. Although Rid argued that – so far – the effects of cyber operations have not in and by themselves constituted 'war', he emphasised that OCCs cause harm through espionage, subversion, and sabotage. Kello introduced the notion of 'unpeace' exactly because the harmful effects of OCCs escaped the normal peaceful relations between states, but did not constitute warfare.[57] And Harknett and Smeets reconceptualised these effects below the threshold of war as cumulatively being able to shift the balance of power, in response to what they saw as a failure to appreciate the strategic impact of OCCs.[58]

Instead, the point we make is that although these scholars insightfully and thoroughly discuss such harms, they nonetheless describe them all as non-violent according to a narrowly physical definition. If there were no analytical utility to expanding the concept of violence, then this point would be purely semantic and so of little theoretical interest. But we argue – and illustrate in detail in subsequent sections – that expanding the concept of violence adds analytical value by providing a useful way to parse different forms of behavior or action even *within* more structural categories of under the threshold competition or unpeace: some violent, some not, and some more violent, others less so, rather than a blanket ascription of non-violence. Importantly, although this discussion has remained within the strategic space of unpeace to highlight the theoretical relevance of the argument, it bears repeating that violent acts occur during peace, unpeace, and war, and so our expansion of the concept of violence can shed further light not only on acts below the threshold of armed conflict, but also acts above this threshold.

Finally, although this narrow conception of violence dominates the literature, it is not a consensus. The above works display internal tensions and disagreements about the relationship of

[53]A search of 'violen* AND cyber' in the the title, abstract, and keywords of major journals with Scopus provides a rough indication of the lack of treatment: in *International Security*; *Strategic Studies*; *and EJIS* only the works already reviewed in this section meet this criterion. For a recent contribution in this journal casting cyber operations as non-violent, see Christopher Whyte, 'Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online', *European Journal of International Security*, 5:2 (2020), p. 201.

[54]See, for example, Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009); Richard J. Harknett and Joseph S. Nye, 'Is deterrence possible in cyberspace?', *International Security*, 42:2 (2017), pp. 196–9; Erik Gartzke and Jon R. Lindsay (eds), *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York, NY: Oxford University Press, 2019).

[55]Erica D. Borghard and Shawn W. Lonergan, 'The logic of coercion in cyberspace', *Security Studies*, 26:3 (2017), pp. 452–81, available at: {https://doi.org/10.1080/09636412.2017.1306396}; Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK and New York, NY: Oxford University Press, 2018).

[56]Liff, for example, is interested in cyber warfare capabilities and concludes that fear of destabilising effects are unwarranted. Adam P. Liff, 'Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war', *Journal of Strategic Studies*, 35:3 (2012), pp. 401–28.

[57]Kello, *The Virtual Weapon and International Order*, pp. 74–8.

[58]Richard J. Harknett and Max Smeets, 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies* (2020), pp. 1–34.

OCCs to violence. Other scholars push against this narrow conception more explicitly. For example, Amir Lupovici recognises that 'the question of whether they [cyber means] are means of violence remains open', while Finlay notes that we 'lack an account of how cyber operations relate to violence' and proceeds to offer an account of violence situated in just war theory.[59] Tim Stevens, in turn, notes that 'affective implications of cyber weapons' should be included, 'which might include feelings of insecurity or fear', but does not theorise this further.[60] We think it is imperative to do so, but before we do so in the third section of the article, we first engage more closely with the literature on violence itself.

Expanding the concept of violence

This section presents an expanded concept of violence, defined as *intentional proximate harm*, focusing on these three aspects in turn: harm, intent, and proximity of means. We understand harm as the diminishing, damage, or destruction of *areas of human value*. We, in turn, identify three general areas of value: the body, affective life, and community. These are neither exhaustive nor generalisable across all times and places, because areas of value are socially and culturally constructed rather than biologically or naturally pre-given.[61] This expanded concept of violence draws on a range of literature on violence in security studies and International Relations more broadly.[62]

The body is the most intuitive locus of harm. However, many forms of bodily pain are learned socially, rather than being an immediate, unmediated sensation. The distinction between bodily harm and harm to one's affective life, which includes psychological or emotional harm, therefore does not imply a 'pure' physicality of the body or a 'non-physical' quality to mental activity.[63] We then distinguish between affective life, which rests at the level of the individual, and community, which captures the value of relations between individuals as well as collective identities, practices, and histories.[64] These areas of value overlap and interact: harm to one can cascade into others, or

[59]Amir Lupovici, 'The "attribution problem" and the social construction of "violence": Taking cyber deterrence literature a step forward', *International Studies Perspectives*, 17:3 (2016), pp. 322–42 (p. 333), available at: {https://doi.org/10.1111/insp.12082}; Christopher J. Finlay, 'Just war, cyber war, and the concept of violence', *Philosophy & Technology*, 31:3 (2018), pp. 357–77 (p. 363), available at: {https://doi.org/10.1007/s13347-017-0299-6}.

[60]Tim Stevens, 'Cyberweapons: An emerging global governance architecture', *Palgrave Communications*, 3 (2017), p. 2. See also Stevens, 'Politics of time', pp. 103–04.

[61]We thus follow Schinkel in focusing on specific 'aspects' of violence. As Schinkel states, 'a choice has to be made explicit concerning the aspects that are selected', otherwise 'alternative ways of defining violence are always more violent than the definition proposed'. Willem Schinkel, *Aspects of Violence* (Basingstoke, UK and New York, NY: Palgrave Macmillan, 2010), pp. 4–13.

[62]Examples of key interventions in this large debate are Vittorio Bufacchi, 'Rethinking violence', *Global Crime*, 10:4 (2009), pp. 293–7, available at: {https://doi.org/10.1080/17440570903248056} and Claire Thomas, 'Why don't we talk about "violence" in International Relations?', *Review of International Studies*, 37:4 (2011), pp. 1815–36, available at: {https://doi.org/10.1017/S0260210510001154}. We heed Krause's caution that 'our understanding of violence is inextricably tied up in what we think we need to know and why'. Keith Krause, 'Beyond definition: Violence in a global perspective', *Global Crime*, 10:4 (2009), pp. 337–55 (p. 338), available at: {https://doi.org/10.1080/17440570903248270}.

[63]Many public health organisations, such as the World Health Organization (WHO) and the US Center for Disease Control, explicitly distinguish emotional and physical harm as different kinds of violence. For a recent discussion, see Karlie E. Stonard, '"Technology was designed for this": Adolescents' perception of the role and impact of the use of technology in cyber dating violence', *Computers in Human Behavior*, 105 (2020), available at: {https://doi.org/10.1016/j.chb.2019.106211}. Similarly, Thomas includes intentionally inflicted psychological harm in her definition of violence; see Thomas, 'Why don't we talk about "violence" in International Relations?', p. 1834. While we follow the broader literature in treating 'physical' and 'bodily' as roughly synonymous in this article, ideally we would move away from the language of physicality altogether, as it implies the existence of a non-physical realm. Psychosomatic conditions demonstrate the complex connection between bodily and mental suffering (all of which is ultimately physical), and so even without the language of physicality this intuitive distinction dissolves on closer inspection – reinforcing our argument for expanding the concept of violence to include both sides.

[64]The WHO defines violence as 'the intentional use of physical force or power, threatened or actual, against oneself, another person, *or against a group or community*, which either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation (our emphasis).' World Health Organization, 'Violence Prevention' (World

characteristics of one can counter harm in others. For example, different harms result from the loss of a limb in communities that are more or less accepting of differently-abled people. Importantly, on this view threats of violence and coercion are themselves violent due to their impact on affective life and community; they create and spread fear and discomfort, and for coercive threats, introduce limits to freedom of action.

This threefold view of value is clearly much broader than the narrow, physical definition of violence in the previous section, but still selective. Fitting with the international security studies focus of this article, the definition is anthropocentric, as it does not include damage to robots, animals, and ecosystems unless that damage affects humans in some way. Similarly, it does not include damage to property or infrastructure unless such damage affects the areas of human value above (which, practically, will often be the case).[65] It also does not follow more ontological concepts of violence in viewing harm as a fundamental 'reduction in being', which is the basis for work on 'dehumanisation' as a violent act.[66]

The breadth of this concept of harm means that there is no lower limit to whether an act is violent. This lack of a lower limit is often captured through the concept of a 'micro-aggression': an act that individually inflicts very little harm, but is nonetheless violent.[67] Consequently, specifying the *severity* of violent action is crucial; however, severity varies massively within and between areas of value and cannot be decided in the abstract.[68] Harm to the community may be commensurable to, or prioritised above, bodily or affective harms, and we consider several examples where this is the case in the following section.

The second aspect of the expanded definition is that violent acts must be *intended* to cause harm. Because only agents, not social structures, can be ascribed intent, our definition excludes 'structural' violence, where harm is caused by social structures such as gender, race, or capitalism.[69] Many discussions of violence treat intention as binary – an act was either intended or not – thus creating conceptual problems regarding accidental or ignorant action and harms that are outside the intended 'target' of violence (for example, 'collateral damage'), or greater/lesser than anticipated. These problems can be sidestepped by treating intention as an agential but still socially ascribed quality (agents exist within specific social contexts), rather than a true purpose 'within' someone's mind. The intention condition then becomes one of reasonable knowledge or foresight that (a specific type, target, or level of) harm would occur.[70]

We limit our discussion of violence to one specific type of agent: the state.[71] We do so acknowledging that political violence includes many non-state actors; indeed, many scholars argue that

Health Organization, 2020), available at: {http://www.who.int/violence_injury_prevention/violence/en/}. Following a similar definition, see Florian J. Egloff, 'Intentions and cyberterrorism', in Paul Cornish (ed.), *Oxford Handbook of Cyber Security* (Oxford, UK: Oxford University Press, 2022).

[65]There is a long history of defining violence in a way that includes 'pure' property damage, following John Locke and political philosophy in the low countries of Northern Europe. See Schinkel, *Aspects of Violence,* p. 27. For an application to OCCs, see the extended discussion, especially the chapter by Simpson with a contrary view, in Luciano Floridi and Mariarosaria Taddeo (eds), *The Ethics of Information Warfare* (Switzerland: Springer International Publishing, 2014), available at: {https://doi.org/10.1007/978-3-319-04135-3}.

[66]See Schinkel, *Aspects of Violence*, esp. pp. 50–1; also Ilan Zvi Baron et al., 'Liberal pacification and the phenomenology of violence', *International Studies Quarterly*, 63:1 (2019), pp. 199–212, available at: {https://doi.org/10.1093/isq/sqy060}.

[67]For recent debate over the definition and scientific applicability of this concept, see the several articles in *Perspectives on Psychological Science*, 12:1 (2017).

[68]In Schinkel's words, 'no general prima facie rule for the severity of violence can be given. This is, after all, not a mathematique sociale.' Schinkel, *Aspects of Violence*, p. 73.

[69]Galtung, 'Violence, peace, and peace research'. We do not mean to deny or downplay such harms, merely to recognise that they are beyond the scope of this article.

[70]Reasonable as judged by a socially constructed 'normal observer'. This is always a contextual issue, but one followed by legal traditions worldwide, even though they differ in setting levels of reasonable anticipation.

[71]Note, we do not limit the applicability of the expanded *definition* of violence by actor, but rather focus our *discussion* of violence on the state.

non-state actors are relatively empowered by cyber capabilities.[72] Added to this, many forms of violence relevant to OCCs (such as gender-based violence involving spyware) are often not directly associated with the state.[73] State violence, however, remains a foundational form in most accounts of OCCs and in political philosophy more widely.[74] Of course, states are not unitary actors and have developed sophisticated practices for collectively committing violent acts. Intelligence, security, and military agencies are the focal point of the most violent actions of the state, and when other state authorities (local municipalities, health and social care, etc.), use violence in extreme cases they rely on the intelligence, security, and military apparatus.

There is a large literature on how states justify their use of violence; however, due to space constraints, we do not address the question of how cyber violence is located within these justifications of violence more broadly.[75] It is nonetheless important to distinguish this question of justification – of the use of violence by states – from issues around the risks and subsequent justification of the conceptual change advocated by this article, which we consider in detail in the following sections.

The third aspect of the expanded definition is proximate means. Harms have many causes on multiple levels, and so we define a violent act as one that intends harm and is a proximate cause of that harm. Although this is partly a temporal matter of immediacy or distance, we recognise that proximate causes can be temporally distant, and more complex notions of causality assign causal weight among different acts using many factors, including the *means* by which harm was inflicted.[76] Although means of violence can be categorised in many ways, the most relevant distinction for OCCs is between material and informational means, or, in other words, how far the infliction of harm depends on the symbolic properties of objects.[77] Material and informational means are not mutually exclusive and the relationship between software and hardware is interdependent: transmitting information relies on certain material properties, while material objects are inconceivable without informational elements.[78] The distinction is, therefore, one of emphasis: whether the material or informational component is the primary way of diminishing or damaging one of the areas of value above.

An example may make the interaction between material and informational means clearer. The effect of armed unmanned aerial vehicles (UAVs) on state violence is another frequently discussed topic.[79] In stark contrast to OCCs, UAVs are usually considered as remote means of inflicting material or kinetic violence, even though the informational infrastructure enabling drones (and also sophisticated missiles) is as complex – and sometimes dependent on similar technologies – to OCCs. This is because UAVs cause harm by dropping bombs on people and

[72]See, for example, Joseph S. Nye, *The Future of Power* (New York, NY: Public Affairs, 2011). Further specifying how cybersecurity interacts with non- and semi-state actors, see Florian J. Egloff, *Semi-State Actors in Cybersecurity* (New York, NY: Oxford University Press, 2022).

[73]Such examples are discussed further in Katharine M. Millar, James Shires, and Tatiana Tropina, 'Gender Approaches to Cybersecurity: Design, Defence and Response' (Geneva: UN Institute for Disarmament Research (UNIDIR), January 2021).

[74]See, for example, the discussion in Elizabeth Frazer and Kimberly Hutchings, 'On politics and violence: Arendt contra Fanon', *Contemporary Political Theory*, 7:1 (2008), pp. 90–108, available at: {https://doi.org/10.1057/palgrave.cpt.9300328}.

[75]They range from no need for state justification (for example, a Schmittian state of exception), through elaborate notions of individual and collective self-defence, to sovereignty- and territory-based claims, as well as polity particular justifications (democratic, theocratic, regime stability, etc.).

[76]Milja Kurki, 'Causes of a divided discipline: Rethinking the concept of cause in International Relations theory', *Review of International Studies*, 32:2 (2006), pp. 189–216.

[77]In Krause's terms, this refers to 'the nature of the act' rather than the 'scale of organization required'. Keith Krause, 'From armed conflict to political violence: Mapping & explaining conflict trends', *Daedalus*, 145:4 (2016), pp. 113–26 (p. 118), available at: {https://doi.org/10.1162/DAED_a_00416}.

[78]See, for example, Samar Faraj and Bijan Azad, 'The materiality of technology: An affordance perspective', in Paul Leonardi, Bonnie A. Nardi, and Jannis Kallinikos (eds), *Materiality and Organizing: Social Interaction in a Technological World* (Oxford, UK: Oxford University Press, 2013).

[79]Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, 'Separating fact from fiction in the debate over drone proliferation', *International Security*, 41:2 (2016), pp. 7–42, available at: {https://doi.org/10.1162/ISEC_a_00257}.

property, whereas OCCs obviously do not. More precisely, for UAVs the causal weight of the missile outweighs that of the command and control infrastructure in the infliction of harm. In contrast, a hypothetical OCC use in a 'critical infrastructure' scenario that caused explosions similar in scale to those of a drone strike would still be an *informational* means of harm, as the symbolic properties of that critical infrastructure (its command and monitoring logics) would have the highest causal weight. However, this scenario requires a more thorough investigation of OCCs based on all three aspects of the expanded definition of violence outlined here – harm, intent, and proximate means – which is the subject of the next section.

Before turning to that section, it is pertinent to review how we have incorporated or deviated from previous work in proposing this expanded definition of violence. Our expanded definition follows a number of scholars and institutions that include psychological harm in the definition of violence.[80] We refined, for example, Claire Thomas's definition, including a more nuanced view of intended harms (that is, our areas of value). We deviated from the WHO definition, as only a more precise conceptualisation (that is, including causal proximity) can clarify the precise way a new means of action, in our case OCCs, should be classified as violent. The merits of such a deviation are shown in the next section.

Rethinking violence and OCCs

This section applies the expanded view of violence set out above to OCCs, arguing that including non-lethal and non-bodily harms means that OCCs relocate, rather than reduce, state violence.[81] More specifically, our threefold view of harm – with the body, affective life, and community as separate areas of value – consolidates several broader views on the harms caused by OCCs.[82]

In an expanded definition of violence, uses of OCCs that are usually considered non-violent, such as website defacement or DDoS, can be violent acts. As indicated above, both *whether* such actions are violent and the *severity* of the violence is extremely context-dependent.[83] For a leisure-based streaming service, forcing people to wait for a website to load might be a minor irritation, while in other cases – Internet voting, denying a minority community a specific language resource or, in the case of the Mirai botnet, depriving whole nations of internet access – this

[80]These are cited throughout the above, exemplary here, Thomas, 'Why don't we talk about "violence" in International Relations?', p. 1834. For OCCs specifically, see Daphna Canetti, Michael L. Gross, and Israel Waismel-Manor, 'Immune from cyberfire?: The psychological and physiological effects of cyberwarfare', in Fritz Alhoff, Adam Henschke, and Bradley Jay Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare* (Oxford, UK: Oxford University Press, 2015).

[81]We draw on a significant body of work outside the strategic studies literature, including David P. Fidler, 'Just & unjust war, uses of force & coercion: An ethical inquiry with cyber illustrations', *Daedalus* (autumn 2016); Massimo Durante, 'Violence, just cyber war and information', *Philosophy & Technology*, 28:3 (2015), pp. 369–85, available at: {https://doi.org/10.1007/s13347-014-0176-5}; and Edward Barrett, 'On the relationship between the ethics and the law of war: Cyber operations and sublethal harm', *Ethics & International Affairs*, 31:4 (2017), pp. 467–77, available at: {https://doi.org/10.1017/S0892679417000454}. See also discussions on violence in the two editions of the 'Tallinn manual' on the use of force and international law in cyberspace.

[82]See, for example, Fabio Cristiano, 'Bodies of cyberwar: Violence and knowledge beyond corporeality', in Althea-Maria Rivas and Brendan Ciarán Browne (eds), *Experiences in Researching Conflict and Violence: Fieldwork Interrupted* (Bristol, UK: Policy Press, 2018). Deibert and Rohozinski's category of risks 'through' (rather than 'to') cyberspace includes 'political opposition and the right to dissent or protest, minority rights and independence movements, religious belief, cultural values, or historical claims'. Ronald J. Deibert and Rafal Rohozinski, 'Risking security: Policies and paradoxes of cyberspace security', *International Political Sociology*, 4:1 (2010), pp. 15–32.

[83]A relatively early debate in the just war literature focused on these distinctions. Randall R. Dipert, 'The ethics of cyberwarfare', *Journal of Military Ethics*, 9:4 (1 December 2010), pp. 384–410, available at: {https://doi.org/10.1080/15027570.2010.536404}. Some authors in this debate maintained a narrow position, suggesting that cyber-blockades could be 'non-violent alternatives'. Neil C. Rowe, 'The ethics of cyberweapons in warfare', *International Journal of Technoethics (IJT)*, 1:1 (2010), pp. 20–31. In later work Rowe addresses civilian 'collateral damage' with an implicit concept of violence that is much broader. Neil C. Rowe, 'Challenges of civilian distinction in cyberwarfare', in Mariarosaria Taddeo and Ludovica Glorioso (eds), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative* (Switzerland: Springer International Publishing, 2017), available at: {https://doi.org/10.1007/978-3-319-45300-2}.

could be a significantly harmful act of violence.[84] Repressive uses of OCCs, which are violent predominantly due to their impact on individuals' affective life (through fear, trauma, and anxiety), and on communities (through 'chilling effects' limiting political speech, and the loss of minority identities),[85] are more likely to be considered violent in an expanded definition, although repressive uses of OCCs have also been connected to bodily violence.[86]

However, our definition of harm implies that some uses of OCCs remain non-violent. The large DDoS attacks that targeted the US financial system in 2012 would only be violent if their impact could be traced to harm to specific individuals or communities. Similarly, the hacker Phineas Fisher's claim that 'in the digital era, robbing a bank [using OCCs] is a non-violent act' is also true *unless* damage is intentionally caused or reasonably foreseen to human bodies, affective lives, or communities.[87] More broadly, Agrafiotis et al.'s 'taxonomy of cyber harm' highlights a range of reputational and economic damage to organisations that, in our view, are only violent if they lead proximately to the diminishment of the three areas of human value above.[88] It is relatively simple to make such a connection for nearly all critical infrastructure cyberattacks. For example, in Matt Sleat's discussion of the 'harm caused to vital human interests through degrading the functionality of computer systems necessary to a country's critical infrastructure' it is not the infrastructure damage *itself* that is violent, but the 'human interests' (bodily, affective, and communal) that are affected.[89]

Other forms of digital harm are excluded from our discussion due to the criterion of intent. Following our bracketing of structural elements of violence in the previous section, we similarly put aside the structural influence of digital technologies. This focus excludes harms created by system-level dynamics in internet governance, such as the economic incentives for writing vulnerable software or weakening encryption technologies to enable state decryption. Furthermore, the intent criterion is an especially complex issue for both interstate and repressive uses of OCCs, because state direction is frequently unclear or indirect. Interstate uses of OCCs often involve proxies and criminal groups, while both interstate and repressive uses rely on private contractors to provide technologies, expertise, and sometimes actual deployment. We recognise that ascribing a clear intent to any specific use of OCCs is a highly complex, time-consuming, and an arduous task; however, this empirical difficulty – and the policy challenges it creates – do not invalidate intent as a conceptual criterion of violence, in cyber or other realms.[90]

[84]Dominic Casciani, 'Briton who knocked Liberia offline jailed', *BBC News* (11 January 2019), available at: {https://www.bbc.com/news/uk-46840461}. Internet shutdowns not caused by OCCs can thus be violent actions, contradicting Asal et al., who classify defacement and DDoS as non-violent protest. Victor Asal et al., 'Repression, education, and politically motivated cyberattacks', *Journal of Global Security Studies*, 1:3 (2016), pp. 235–47, available at: {https://doi.org/10.1093/jogss/ogw006}.

[85]Ron J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Plattsburgh, NY: Signal Books, 2013); Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018).

[86]Anita R. Gohdes, 'Studying the Internet and violent conflict', *Conflict Management and Peace Science* (2017); Nils B. Weidmann and Espen Geelmuyden Rød, *The Internet and Political Protest in Autocracies* (New York, NY: Oxford University Press, 2019).

[87]Lorenzo Franceschi-Bicchierai, 'Phineas Fisher offers $100,000 bounty to hack banks and oil companies', *Vice* (17 November 2019), available at: {https://www.vice.com/en_us/article/vb5agy/phineas-fisher-offers-dollar100000-bounty-for-hacks-against-banks-and-oil-companies}. On Fisher's background and justification for his actions, see Joseph Menn, *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World* (New York, NY: PublicAffairs, 2020), pp. 165–72.

[88]Ioannis Agrafiotis et al., 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cybersecurity*, 4:1 (2018), available at: {https://doi.org/10.1093/cybsec/tyy006}.

[89]Matt Sleat, 'Just cyber war?: Casus belli, information ethics, and the human perspective', *Review of International Studies*, 44:2 (2018), pp. 324–42 (p. 326), available at: {https://doi.org/10.1017/S026021051700047X}. See also Thomas W. Smith, 'The new law of war: Legitimizing hi-tech and infrastructural violence', *International Studies Quarterly*, 46:3 (1 September 2002), pp. 355–74, available at: {https://doi.org/10.1111/1468-2478.00237}.

[90]The classic example of difficulties in establishing intention to harm – and adequate justifications for harm – is medical ethics, but this comparison, although theoretically interesting, is outside our scope.

The third aspect of the expanded definition of violence is proximate means, treated briefly in the contrasting comparison with armed UAVs at the end of the previous section. Cyber capabilities, as information systems, alter information (although through material networks), and so their capacity for violence is based on the added possibility of devaluing areas of value through informational means as well as or instead of material ones. This distinction is not always easy to draw: a pacemaker cyberattack that uses code to affect an individual's heart function clearly depends on symbolic properties, while the categorisation of a GIF that induces a seizure is not so obvious because the strobe light inducing epilepsy is not symbolic.[91] Stuxnet also demonstrates the impossibility of completely disentangling informational and material means: the virus damaged centrifuges by altering their rotational speed and pressure sensors, but its success depended on many material objects, from the test centrifuges constructed in the US to the USB drive physically carried by an agent into the enrichment facility.

Nonetheless, the ability of OCCs to inflict harm through informational means opens up a category of 'non-kinetic' violence, which furthers the insights of the strategic studies scholarship reviewed above.[92] These scholars also see proximity as a crucial aspect of OCCs: Rid suggests that harm from OCCs is 'mediated, delayed and permeated by chance and friction', while for Kello cyber-attacks 'lack a proximate cause of injury'.[93] The expanded definition proposed here implies that OCCs can be sufficiently proximate to constitute violent acts despite their causal complexity. As explained in the previous section, sufficient proximity is a causal rather than geographic criterion, as OCCs can be operated with a reasonable certainty of effect from a vast distance.

To demonstrate the analytical value of expanding the concept of violence to distinguish between different kinds of under-the-threshold cyber operations, the remainder of this section provides illustrative examples in each of Rid's three categories of espionage, sabotage, and subversion. Within these categories, an expanded concept of violence usefully reorders the analytical space, helping us to understand and prioritise the range of harmful effects involved.

First, an expanded concept of violence requires us to reassess the harms caused by different forms of cyber-espionage. State-sponsored industrial or commercial cyber-espionage is unlikely to fulfil any of the three aspects of violence above: first, it often harms organisations rather than humans, especially property (including intellectual property); second, it is not usually 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 (such as the transfer of patent designs) is sufficiently proximate to satisfy the third condition.[94]

In contrast, cyber-espionage in repressive contexts, directly violating individual rights of privacy and indirectly creating 'chilling effects', may well meet our expanded criteria of intentional proximate harm on both affective and community levels. While espionage networks to spy on diaspora communities predate the Internet, they are relatively costly, tedious to maintain, and difficult to establish globally. Cyber capabilities transform this calculation, and potentially offer the home state an easy pathway to achieve global reach. The use of OCCs for repression would be

[91]Reis Thebault, 'A tweet gave a journalist a seizure: His case brings new meaning to the idea of "online assault"', *Washington Post* (17 December 2019), available at: {https://www.washingtonpost.com/health/2019/12/16/eichenwald-strobe-gif-seizure-case/}.

[92]On 'non-kinetic', see Finlay, 'Just war, cyber war, and the concept of violence', p. 370.

[93]Rid, 'Cyber war will not take place' (2012), p. 9; Kello, 'The meaning of the cyber revolution', p. 24. Rid expands further on the 'indirect' violence of OCCs in 'More attacks, less violence', where he states that 'violence administered through computer code, as a result of its indirect nature, is bound to remain unqualified' (p. 140). Rid's definition of 'qualified' here is complex, but essentially refers to the institutionalisation, even naturalisation, of state violence. For Rid, state power and force always, at their heart, involve bodily violence, and OCCs must therefore be somewhat external to this process.

[94]For further argument regarding the difficulties in relating cyber-espionage directly to harm or economic disadvantage, see Gilli and Gilli, 'Why China has not caught up yet'.

non-violent in a narrow definition unless directly linked to arbitrary detention and torture. This conceptualisation is one of the reasons that advocacy groups and international human rights representatives have sought to tie commercial spyware identified on the devices of Saudi dissident Omar Abdulaziz and others to the murder of Jamal Khashoggi in the Saudi consulate in Istanbul in October 2018.[95]

However, digital censorship and surveillance could also be conceived as relocated state violence. When individual 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). Examples for such operations are plentiful and well documented, for example in the case of the Tibetan or Uighur minorities.[96] For surveillance, an expanded definition of violence including affective and psychological impacts would help to mobilise policy discussions on the regulation of commercial spyware to repressive states, without requiring specific instances of bodily harm to be associated with their use.

Second, regarding sabotage, a good illustration of the impactful use of OCCs is NotPetya, destructive malware originally spread via Ukrainian tax software.[97] Its initial infection, attributed to the Russian military intelligence directorate (GRU), led to a disruption of Ukrainian government functions in the context of Russian occupation of the Crimean Peninsula and the Donbas region, followed by global spread into a wide range of major multinational firms. In a narrow definition of violence, this would be non-violent as it did not cause bodily harm or death. The apparently non-violent yet impactful character of NotPetya has left scholars and policymakers struggling to capture its effects.

However, NotPetya is violent in an expanded definition, though the intent of the attackers is crucial in judging 'how violent' and consequently calibrating the policy response. At a more limited level, NotPetya could be interpreted as designed specifically to erode confidence in Ukrainian society, economy, and trust in the state, creating a collective feeling of vulnerability and causing harm at a community level. The malware was 'designed to send a political message: If you do business in Ukraine, bad things are going to happen to you.'[98] In this reading, extensive international effects were collateral damage to the country-focused operational intent.[99] A contrasting judgement sees NotPetya's authors as fully culpable for intentionally producing global damage, knowing the malware would spread outside Ukraine. In this view, NotPetya was a carefully considered device for strategic signalling worldwide, using the destabilisation of global economic actors as a medium to send the message.[100] We do not seek to decide between these alternative interpretations here, but stress that, on an expanded definition of violence, both accounts are describing violent acts, though the second is more severe than the first as the intent covers a

[95]Bill Marczak et al., 'The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil' (Citizen Lab, 1 October 2018); Agnes Callamard and David Kaye, 'UN Experts Call for Investigation into Allegations That Saudi Crown Prince Involved in Hacking of Jeff Bezos' Phone', United Nations Office of the High Commissioner for Human Rights (22 January 2020), available at: {https://perma.cc/EFY4-KZQX}.

[96]See, for example, Citizen Lab, 'Targeted Threats', Citizen Lab Website (2021), available at: {https://perma.cc/G74G-BFEY}.

[97]In 'More attacks, less violence', Rid distinguishes between two views of sabotage: the now standard view where sabotage can include kinetic disruption, and a narrower historical understanding where sabotage is only temporary disruption, which 'has nothing to do with violence, neither to life nor to property' (p. 141, quoting Giovannitti). Rid suggests that OCCs 'restrain violence and make that line easier to draw' (p. 141), and so would likely simply consider NotPetya non-violent, foregoing the range of analytical options discussed here.

[98]Craig Williams quoted in Greenberg, *Sandworm*, p. 213.

[99]See, for example, 'Ukraine was clearly the central target', in Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), p. 300.

[100]Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, 'Cyberwarfare has taken a new turn: Yes, it's time to worry', *Washington Post* (13 July 2017), available at: {https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyberwarfare-has-taken-a-new-turn-yes-its-time-to-worry/}.

wider area of harm. Either way, this use of offensive cyber capabilities relocates interstate violence, by debilitating the affective lives of individuals and inflicting harm on communities.

Third, regarding subversion, OCCs have been frequently deployed in what are known as 'hack-and-leak' operations, where sensitive information is obtained through a cyber intrusion and then published online. The paradigm example is the compromise of the US Democratic National Committee (DNC) by the Russian military intelligence agency, the GRU, during the 2016 presidential elections, but such operations are far more widespread.[101] As a combination of OCCs with broader techniques of information and influence operations, hack-and-leaks are highly relevant to under-the-threshold state competition, but clearly not violent on a narrow definition. Moving to an expanded definition of violence, in contrast, helps us distinguish between hack-and-leaks that directly cause affective harms by publishing private personal data (kompromat) and so are violent, and those that leak affectively neutral but strategically valuable organisational capabilities, which are not. Empirical examples in the former, violent, category include reported operations against Al-Jazeera anchor Ghada Oueiss and the Sony Pictures Entertainment executive Amy Pascal, while ones in the latter, non-violent, category include the Shadow Brokers releases of US OCCs, and the leak of NHS documents before the 2019 UK general election.[102]

Overall, this section has argued that OCCs can be violent even though we agree with the strategic studies literature that it is difficult, though not impossible, for them to cause bodily harm (and especially *lethal* bodily harm). An expanded concept of violence highlights non-bodily affective and communal harms caused by OCCs, suggesting that OCCs *relocate* rather than reduce violence. It therefore adds analytical value to current insights of strategic studies on the kinds of harm caused by cyber operations, parsing more finely different forms of espionage, sabotage, and subversion. It also emphasises that violent uses of OCCs are likely to occur in repressive situations, while canonical forms of cyber-espionage remain non-violent. Furthermore, the examples in this section underline that interference with data in a digitalised society may result in harm commensurate with or exceeding the destruction of physical objects or bodily injury.[103] Consequently, capturing affective and community harms as violence is not only analytically useful, but also normatively consequential, and we return to the policy implications of this shift in the conclusion. Before doing so, we consider the risks of this conceptual expansion.

The risks of conceptual expansion

There are several downsides of an expanded concept of violence in relation to OCCs, of which we address three in this section: manipulation, legal implications, and a consequent lack of focus. We see these three downsides as representing real risks, but nonetheless conclude that the analytical benefits above, combined with the policy benefits considered in the concluding section, outweigh these risks.

First, there is the question whether an expanded concept facilitates political and ideological exploitation, particularly as it does not have a lower threshold of harm. The risk of exploitation in this manner can be illustrated by the trajectory of the related concept of 'cybercrime'. Although early international agreements on cybercrime, such as the 2001 Budapest Convention, sought to circumscribe the concept to cover only economic transgressions – fraud, identity theft, and so on

[101]See, for example, James Shires, 'Hack-and-leak operations: Intrusion and influence in the gulf', *Journal of Cyber Policy*, 4:2 (2019), pp. 235–56; James Shires, 'The simulation of scandal: Hack-and-leak operations, the Gulf States, and U.S. politics', *Texas National Security Review*, 3:4 (2020).

[102]For Shadow Brokers, this evaluation considers the leak itself, not the subsequent reuse of such capabilities afterwards. For Sony Pictures and Shadow Brokers, see Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020). On Oueiss, see Ghada Oueiss, 'I'm a female journalist in the Middle East: I won't be silenced by online attacks', *Washington Post* (8 July 2020). On the NHS documents, see Dan Sabbagh, 'Leaked NHS dossier inquiry focuses on personal Gmail accounts', *The Guardian* (19 December 2019).

[103]A view also supported by the ICRC; see 'International Humanitarian Law and Cyber Operations During Armed Conflicts', position paper, International Committee of the Red Cross (ICRC) (Geneva, 2019).

– many national laws later expanded the concept to 'content' crimes, such as posting politically or socially undesirable content online.[104] This expansion, which provides repressive regimes with a new lever of information control, has begun to supplant the narrower definition of the Budapest Convention internationally.[105]

Such manoeuvres should of course be tracked carefully to assess the consequences of conceptual manipulation for both established definitions and proposed alternatives. More specifically, one could expect an authoritarian state to target political opponents by using an expanded definition of violence to claim that cyber operations harming – for example – national unity are violent cybercrimes, and so should be punished accordingly. This article has argued that there are many violent (that is, intentional and proximate) uses of OCCs that cause harm to national or other communities, and so calling such action violent would not necessarily be misleading.[106] Even so, a repressive response against the perpetrators would likely be highly disproportionate to the initial harm, and so unjustified. As indicated earlier, state justifications for violence are outside the scope of this article, and so the justification of repressive violence through the identification of earlier violent uses of OCCs – although important – is also beyond the scope of our discussion.

Another downside is the potential implication of conceptual expansion on (international) legal understandings of armed conflict. Though such an impact is unlikely, as it would presuppose that our proposed expansion be broadly accepted by the international legal community and the community of states, we briefly anticipate such implications.

There are two major international legal frameworks that an expanded concept of violence for OCCs could affect: *jus ad bellum*, particularly its understandings of use of force and armed attack, and *jus in bello*, particularly international humanitarian law's (IHL) focuses on violence and the protection of civilians during armed conflicts. For the former, the expanded concept of violence may lead to more cyber operations being considered a use of force than a narrow conception.[107] Even then, an expanded concept of violence is unlikely to have any impact on the definition of 'armed attack', which is generally considered to be a higher threshold, depending on the scale and effects of the operation compared to physical precedents.[108] Importantly, when scholars speak about sub-threshold activity, they usually mean the threshold of armed conflict, which is determined by whether an 'armed attack' has occurred. Thus, although an expanded definition of violence implies more sub-threshold activity is violent (and potentially a use of force), it is highly unlikely to move the threshold itself.

With regard to *jus in bello*, it is important to note that IHL may apply before the notion of 'armed attack' has been reached, as IHL uses a different, 'armed force', criterium for its

[104]See, for example, James Shires, 'Ambiguity and appropriation: Cybercrime in Egypt and the Gulf', in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Power, Behavior, and Diplomacy* (London, UK: Rowman & Littlefield Publishers, Inc., 2020), pp. 205–26; Shires, *The Politics of Cybersecurity in the Middle East*, ch. 4.

[105]Russian proposals for a new treaty on cybercrime in 2019 – incorporating content concerns – are likely to dominate cybersecurity governance negotiations at the UN in the upcoming years.

[106]Of course, the potential for exploitation partly depends on the truth of the claim. Where such claims are false, this is no more than one pretext for repression among many others.

[107]The first Tallinn manual provides eight criteria to judge whether a cyber operation is a use of force: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality. The first, third, and fourth criteria are potentially open to more permissive interpretations based on an expanded concept of violence, while the second (immediacy) is akin to the proximity criterion in the expanded conception. For more detail, see, for example, Michael N. Schmitt, 'The use of cyber force and international law', in Marc Weller, *The Oxford Handbook of the Use of Force in International Law* (Oxford, UK: Oxford University Press, 2015). For a more general discussion, see Tom Ruys, 'The meaning of "force" and the boundaries of the "jus ad bellum": Are "minimal" uses of force excluded from UN Charter Article 2(4)?', *The American Journal of International Law*, 108:2 (2014), pp. 159–210.

[108]Nicaragua judgement, International Court of Justice. Note that the United States has not followed that interpretation and considers there to be no difference between 'use of force' and 'armed attack'. See NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge, UK: Cambridge University Press, 2017), Rule 69.

applicability.[109] Many IHL rules start with the notion of an 'attack', defined by Article 49 AP I of the Geneva Conventions as 'acts of violence against the adversary, whether in offence or in defence'.[110] As for what constitutes violence, IHL would include death, injury, and physical damage, with some states and institutions also including 'harm due to the foreseeable indirect (or reverberating) effects of attacks'.[111] The ICRC has argued that 'an operation designed to disable a computer or a computer network during an armed conflict constitutes an attack as defined in IHL whether or not the object is disabled through destruction or in any other way.'[112] A too narrow reading would lead to the unsatisfactory result of logical but not destructive operations against civilian networks not being covered by IHL. Consequently, the ICRC authors argue that adopting an expanded concept of violence 'constitutes one of the most critical debates for the protection of civilians against the effects of cyber operations'.[113]

It is thus very clear that as a matter of IHL, a broader notion of violence leads to more protection against more acts for more people. Our proposition of the expanded definition of violence goes in the same direction as some of the expert commentary in international law.[114] However, just as different bodies of law have different notions of 'attack', different bodies of law have different criteria for what they consider the threshold to be for relevant acts of 'violence'. Our analytical concept is in no way meant to be determinative for the international legal understandings of the term.

The third potential downside of conceptual expansion is to diminish the association of the concept of violence only with bodily harm by adding intentional proximate causes of affective and community harms. Some scholars diagnose this problem in the broader literature on violence, disagreeing sharply with the works reviewed in the section on the concept of violence above. For example, Stathis N. Kalyvas recommends keeping violence restricted to physical harm for fear of diluting the focus of political science on what constitutes an important and already diverse category of human behaviour.[115]

Crucially, because violence is a normative as well as analytical concept, implicit in this view is an *a priori* prioritisation and condemnation of bodily over affective and community harm, which we reject. Even if we relied on other words such as harm, cost, or damage, instead of expanding the concept of violence – and specifying the qualities of intention and proximity each time – the normative connotations of violence would be absent from affective and community harms, reinforcing this instinctive prioritisation. We believe that this should not be a definitional matter but one of empirical investigation: in specific contexts, all of which are violent, what were the exact harms inflicted, and how were they experienced by those who were subject to them? We have sought to mitigate the risk of a lack of focus in this article by stressing the context-dependence of comparison between different kinds of harm, especially in the case of cyber operations. Insofar as scholarly and policy focus shifts as a result, this is not a conceptual error but an overdue recognition of the variety of harms humans can experience. In the conclusion of the article, we return to the benefits of our argument for policy, as well as theory, on OCCs.

[109]Note: the threshold for 'armed force' is debated both physically and with cyber means. See Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts', *International Review of the Red Cross*, 102:913 (2020), p. 304; NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 82.

[110]Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

[111]Gisel, Rodenhäuser, and Dörmann, 'Twenty years on', p. 313.

[112]Ibid.

[113]Ibid., p. 314.

[114]Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford, UK: Oxford University Press, 2014), p. 181.

[115]Stathis N. Kalyvas, 'The landscape of political violence', in Erica Chenoweth et al. (eds), *The Oxford Handbook of Terrorism* (New York, NY: Oxford University Press, 2019), p. 13.

Conclusion: Relocating violence, rethinking policy

The transformation and reinvention of state violence has continued into the digital age. The clearest manifestation of state violence in cyberspace is in offensive cyber capabilities: the adversarial manipulation of digital devices and networks for interstate competition and globalised repression. However, the literature on OCCs is dominated by a narrow definition of violence as bodily harm, classifying OCCs as largely non-violent. This narrow definition has both analytical and policy consequences. Analytically, it implies undue homogeneity across the wide range of strategically relevant uses of OCCs. At a policy level, it means that many harms caused by OCCs are un- or under-appreciated by states and other actors.

The account provided here provides greater analytical purchase on this expanding domain, as well as stronger normative foundation for action. An expanded concept of violence, including affective and community harms, reveals how OCCs *relocate* state violence through new means of repression and information manipulation, without simplifying or exaggerating their complex effects. Some readers may object that expanding the definition of violence is hazardous, diluting the devastating effects violent actions have on their victims and their communities. While we recognise this danger, we aim to show that the opposite is also true. Holding on to a narrow definition of violence leads one to misconstrue the harms resulting from the use of OCCs to the detriment of their victims.

Further research is required to substantiate this relocation with empirical data, including large-scale surveys of cyber conflict and extended case studies that trace the decision-making processes behind individual deployments. Further work is also needed to transfer this account of violence from states to semi- and non-state actors, as well as to examine the justifications for violent uses of OCCs in more detail.

This article has three main implications for theory and policy on cyber conflict. First, the affective and community harms caused by OCCs need to be identified, anticipated, and taken seriously in decisions about their use. Second, research and policy should focus on the most violent uses of OCCs, which may not be state-sponsored cyber-espionage or sabotage, but instead the adaption of authoritarian systems to rely on digital and globalised repression and rework existing practices of information manipulation against their adversaries. Third, and most importantly, adherence to a narrow conception of violence means that many states have undertaken significant harmful actions in their own and each other's societies without recognising them as such. Our current conceptual tools hamper institutional adaptation to counter and mitigate these broader harms, such as military doctrines and capabilities, intelligence capabilities, criminal laws, police support, victim counselling, and so on. Our redrawing of the concept of violence to include affective and community harms provides defensive actors with a stronger conceptual foundation to accurately measure harms exerted via digital means and then act to prevent them.

Are OCCs the better angels of our digital nature? We have argued that they are not; on an expanded concept of violence, OCCs represent not Pinkerian optimism, but a more complex relocation of state violence. The main contribution of this article is thus the application of an expanded conception of violence to better understand the impact of OCCs on individuals and societies. But the account of violence put forward here also has broader implications. Many other emerging security technologies, such as lethal autonomous weapons systems, raise similar questions about the extent and type of violence they cause, in part due to their reliance on informational as well as material means to produce harmful effects. The expansion of the concept of violence we have undertaken in this article could also be applied to other information-enabled technologies, to identify and ultimately work to ameliorate currently unseen forms of harm in global politics. Consequently, in addition to its main contribution in rethinking the violence involved in cyber conflict, our study also provides new insights into how to best conceptualise violence in international affairs more widely.

Acknowledgements. 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 to the Digital Democracy Workshop organised by the Digital Democracy Lab at University of Zurich in November 2020. We thank all participants for their helpful feedback.

Florian J. Egloff is a Senior Researcher in Cybersecurity at the Center for Security Studies (CSS) at ETH Zurich. His publications focus on the role of non- and semi-state actors in cybersecurity, the politics of public attribution, and the use of cyber intrusions for political purposes. He is the author of the forthcoming book *Semi-State Actors in Cybersecurity* (Oxford University Press, 2022). Author's email: florianegloff@ethz.ch. Twitter: @egflo

James Shires is an Assistant Professor in Cybersecurity Governance at the Institute of Security and Global Affairs, University of Leiden. He is a Fellow with The Hague Program for Cyber Norms and the Cyber Statecraft Initiative at the Atlantic Council. He has written widely on issues of cybersecurity and international politics, including on cybersecurity expertise, digital authoritarianism, spyware regulation, and hack-and-leak operations. He is the author of *The Politics of Cybersecurity in the Middle East* (Hurst/Oxford University Press 2021). Author's email: j.shires@fgga.leidenuniv.nl. Twitter: @jamessshires

Cite this article: Egloff, F. J., Shires, J. 2021. The better angels of our digital nature? Offensive cyber capabilities and state violence. *European Journal of International Security* X: 1–20. https://doi.org/10.1017/eis.2021.20