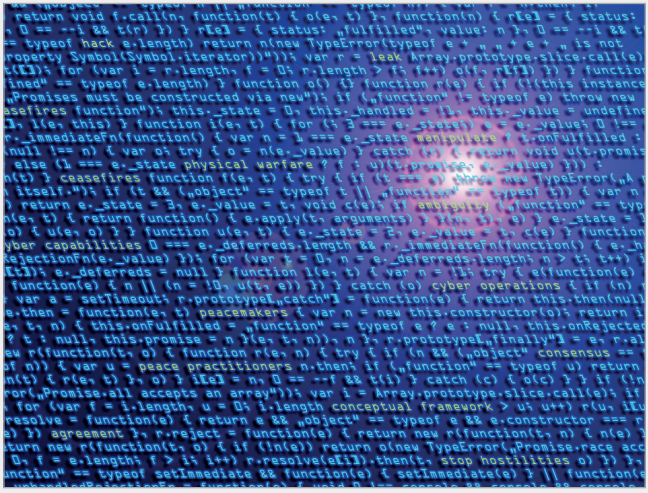
CSS MEDIATION RESOURCES

Cyber Ceasefires: Incorporating Restraints on Offensive Cyber Operations in Agreements to Stop Armed Conflict

Sean Kane and Govinda Clayton



CSS ETH Zürich

ETH zürich

Sean Kane has worked on mediation processes and political dialogues related to political transitions, elections, and territorial disputes for the UN, the United States Institute of Peace, and the Centre for Humanitarian Dialogue in Iraq, Libya, Afghanistan, and Syria. He currently works for the UN's Mediation Support Unit and is a graduate of the Master of Advanced Studies ETH Mediation in Peace Processes (MAS ETH MPP) program hosted by ETH Zurich.

Govinda Clayton is Senior Researcher in peace processes at the Center for Security Studies (CSS) at ETH Zurich. In his work, he combines research, teaching, and practice to transform communication and conflictual dialogue between individuals and groups, to help bridge differences, and to heal political divides. He currently leads the Ceasefires Project, generating knowledge and practical guidance on how to negotiate and implement ceasefires during intra-state conflict.

Center for Security Studies (CSS)
Swiss Federal Institute of Technology, ETH Zurich
Haldeneggsteig 4. IFW CH – 8092 Zurich
Tel: +41 33 632 40 25
mediation@sipo.gess.ethz.ch
www.css.ethz.ch

Copyright front cover picture: Miriam Dahinden-Ganzoni
Editor: Simon J. A. Mason
English copy-editing: Michael Woods
Layout: Miriam Dahinden-Ganzoni
Available online at: www.css.ethz.ch as a pdf, or order a hard copy by email mediation@sipo.gess.ethz.ch

Acknowledgements: The authors would like to thank all of the cyber experts (Max Smeets (CSS), Myriam Dunn Cavelty (CSS), Florian Egloff (CSS), Lennart Maschmeyer (CSS), Jakob Bund (CSS), James Shires (Leiden University), and Camino Kavanagh (Kings College London), ceasefire and mediation experts (Julian Th. Hottinger (FDFA), Georg Stein (FDFA), and Ajay Sethi (UN)), and mediation experts (Simon J. A. Mason (CSS), Teresa Whitfield (UN), Asif Khan (UN) and Enrico Formica (UN)) for helpful conversations and comments that have greatly improved this paper. Thanks also to Julia Schlosser (CSS) for research assistance and Michael Woods for copy-editing. The financial support of the Swiss Federal Department of Foreign Affairs (FDFA), in the framework of the Mediation Support Project (a joint project of the Center for Security Studies at ETH Zurich and swisspeace), is gratefully acknowledged. Govinda Clayton also acknowledges the financial support of the Swedish Research Council [2018-01520].

ISSN: 2296-7397
ISBN: 978-3-905696-80-6
DOI: 10.3929/ethz-b-000491263

Cyber Ceasefires: Incorporating Restraints on Offensive Cyber Operations in Agreements to Stop Armed Conflict

Sean Kane and Govinda Clayton

CSS
ETH Zürich

ETH zürich

Content

Summary

Offensive cyber capabilities involve the use of a combination of technological, human, and organizational resources to manipulate, hack, damage, or destroy digital services or networks (Egloff & Shires, 2020). There is a growing convergence between offensive cyber capabilities and physical warfare. As the International Committee of the Red Cross (ICRC) recently proclaimed, cyber operations are now a "reality in contemporary armed conflict" (ICRC, 2019: 2).

Yet despite the increased use of offensive cyber capabilities in armed conflict, there does not yet exist any guidance for peace practitioners on if, or how, peace processes may need to evolve with this trend. This paper represents one of the first attempts to address this lacuna, focusing specifically on how developments in offensive cyber capabilities might impact efforts to negotiate and implement ceasefires. It also sets out and analyzes possible adaptations and responses.

Ceasefires are arrangements during armed conflict whereby at least one conflict party commits to cease hostilities from a specific point in time (Clayton et al., 2019). The ceasefire negotiation process is where conflict parties, often supported by peacemakers, devise an approach to cease hostilities and manage the specific military technologies used in the conflict. Effective agreements tend to specify the prohibited behaviors in all relevant forms of warfare. Where cyber operations have featured in an armed conflict, a potentially hazardous ambiguity is created by a failure to prohibit certain offensive cyber capabilities clearly or to put in place structures to manage and resolve incidents that arise in cyberspace during the implementation of a ceasefire. This is especially the case given the still evolving military application of these capabilities and the lack of consensus as to when the effects of a cyber operation rise to the threshold of an armed attack, creating ample room for miscalculation by conflict parties. The authors provide three recommendations to aid peace practitioners involved in designing talks to stop hostilities:

1. *Conflict analysis:* Conflict analysis undertaken prior to a ceasefire negotiation should assess the presence or absence of offensive cyber capabilities and operations in the conflict landscape.

2. *Process design:* Where and when offensive cyber operations pose a salient threat to the stability of a prospective ceasefire, they should be incorporated into the negotiations process design.

3. *Provisions and conceptual frameworks:* When conflict parties opt to incorporate a restraint on cyber operations into a ceasefire agreement, agreeing on the broad goal of the cyber dimension of the ceasefire could help determine a suitable cyber ceasefire conceptual framework and associated technical provisions. The authors propose four possible options for cyber ceasefire conceptual frameworks ("Acknowledgement," "Constraint and Coordination," "Comprehensive Management," and "Cooperation") as well as combinations of associated technical provisions.

1. Introduction

There is a growing convergence between cyber activities and physical warfare. However, despite the increased use of offensive cyber capabilities in armed conflict, there is still no guidance for peace practitioners on if, or how, peace processes may need to evolve with this trend. Academic literature is similarly underdeveloped in this area. This paper is, to the best of our knowledge, the first effort to address this lacuna. It focuses specifically on how developments in offensive cyber capabilities might impact efforts to negotiate and implement ceasefires, and it sets out and analyzes possible adaptations and responses.

Offensive cyber capabilities involve the use of a combination of technological, human, and, organizational resources to manipulate, hack, damage, or destroy digital services or networks (Egloff & Shires, 2020). They are increasingly being used as a tool to engage in or accompany physical warfare. For example, in recent years, we have observed cyberattacks targeting critical infrastructure as part of the ongoing conflict in Ukraine (Greenberg, 2017), the Israel Defense Forces destroying a building in Gaza that allegedly housed Hamas's cyber command (Newman, 2019), US airstrikes killing alleged hackers from the so-called Islamic State in Syria (Ackerman, MacAskill & Ross, 2015), and several governments shutting down internet networks to gain a tactical advantage during military operations in contested (internal) regions (Gohdes, 2015). While cyber operations have been part of strategic military planning since the 1990s (e.g., the US Department of Defense's 1997 "Eligible Receiver" and 1999 "Zenith Star" exercises), advances in technology mean an increasing number of diverse conflict parties now treat cyberspace as a domain of warfare. As the International Committee of the Red Cross (ICRC) recently proclaimed, cyber operations are now a "reality in contemporary armed conflict" (ICRC, 2019: 2). Their military use is only expected to expand (United Nations, 2021: 3).

Despite these developments, there remains a lack of consensus regarding the military effectiveness of offensive cyber capabilities during armed conflict. Of the few empirical studies that exist on this issue, a number call into question the widespread viability and efficacy of these new cyber tools (Gartzke, 2013; Lindsay, 2017; Maschmeyer, 2020). This leaves scholars of cyber conflict with a dilemma "overstate the potential lethal and physical harm caused by offensive cyber capabilities in order to secure policy-makers' attention", or characterize cyber capabilities as mostly non-violent, compar-

atively insignificant and risk overlooking the effect that they can have on the course of current and future conflicts (Shires & Egloff, 2020). We counsel against this binary framing. The introduction of a new mode of conflict, even if limited in scope and effect, is important to consider from the perspective of the peace process, in particular with regards to the stability of ceasefires.

Ceasefires are publicly announced arrangements during armed conflict whereby at least one conflict party commits to cease hostilities (and potentially other defined behaviors) from a specific point in time (Clayton et al., 2019). Conflict parties use ceasefires to address violence before, during, and at the conclusion of negotiations around the broader set of contested political and security issues (Brickhill, 2018). The ceasefire negotiation process is where peacemakers and the conflict parties devise an approach to cease hostilities and manage the specific military technologies used in the conflict. For almost two decades, practitioners have consistently held that specificity and detail are paramount to the success of a ceasefire (Haysom & Hottinger, 2004; Potter, 2004; United Nations, forthcoming). Thus, effective agreements tend to specify the prohibited behaviors in all relevant forms of warfare, and they put in place structures to manage and resolve any subsequent incidents or violations.

Particularly where cyber operations have featured in an armed conflict, a potentially hazardous ambiguity is created by a failure to prohibit certain offensive cyber capabilities in a clear way or to put in place structures to manage and resolve incidents that arise in cyberspace during implementation of a ceasefire. In particular, the difficulties in attributing responsibility for cyber operations, and the capacity of these tools to inflict a range of physical, economic, and political costs on adversaries, represent new and important risk factors to the stability of ceasefire regimes.

In order to aid peace practitioners called upon to respond to this new aspect of contemporary conflict, we make three key recommendations in relation to designing talks to stop hostilities:

1. *Conflict analysis:* Conflict analysis undertaken prior to a ceasefire negotiation should assess the presence or absence of offensive cyber capabilities and operations in the conflict landscape.

2. *Process design:* Where and when offensive cyber operations pose a salient threat to the stability of a prospective ceasefire, they should be incorporated into the negotiations process design. This could occur as part of the

main ceasefire negotiations or as a separate sub-committee dedicated to the cyber-dimension. In either case, this could require the involvement of technical experts from the conflict parties and possibly private network actors, cyber incident responders, and implicated international actors.

3. *Provisions and conceptual frameworks:* When conflict parties opt to incorporate a restraint on cyber operations into a ceasefire agreement, agreeing on the broad goal of the cyber dimension of the ceasefire could help determine a suitable cyber ceasefire conceptual framework and associated technical provisions. We propose four possible options: "Acknowledgement," "Constraint and Coordination," "Comprehensive management," and "Cooperation".

In what follows, we first discuss offensive cyber capabilities, providing basic definitions, illustrating their extant use in armed conflict, and exploring which categories of capabilities may be most relevant to ceasefire agreements. We underscore here that our main interest is in the deployment of offensive cyber capabilities in armed conflict and not their use in other contexts, such as the so-called "grey zone" between peace and war. In our discussion, we do, however, cite some examples of cyber operations conducted outside situations of armed conflict if they are a particularly clear illustration of a certain capability or are generally considered a landmark case. Second, we provide a brief overview of the current practice of ceasefires in armed conflict, defining key terms and offering a basic description of the functions and contents of ceasefire agreements. Third, we make an initial attempt to examine the prospective incorporation of restraints on offensive cyber capabilities into ceasefires. In doing so, we set out why this is necessary, outline associated challenges, and propose practical options for how restraints on cyber capabilities could be reflected in broader ceasefire agreements.

2. Offensive Cyber Capabilities

2.1. What Are Offensive Cyber Capabilities?

The term offensive cyber capabilities can have a variety of different meanings (Shires & Smeets, 2017). We follow Egloff & Shires (2020) in defining them as a combination of technological, human, and organizational features that jointly enable the adversarial manipulation of digital services or networks. The benefit of this definition is that it does not focus on the technical details of the software elements or techniques undergirding the offensive capability but rather the intended impact or effect of their use: adversarial manipulation (i.e., using tools in a manner against the target's interests) (Egloff & Shires, 2020). In practice, the goal of this manipulation can be to disrupt, deny, degrade, deceive, or destroy adversaries' access to a system or network or to extract protected or confidential data from such networks (Bodeau & Graubard, 2013; Bellovin, Landau & Lin, 2017; Smeets, 2018: 93). Rather than present an exhaustive list of all types of offensive cyber capabilities, we briefly discuss the most common goals of adversarial manipulation and highlight their use in, and potential relevance to, armed conflict. We focus on four categories of goals, which we present in table 1. Notably, as we discuss below, not all of these categories of offensive capabilities are well-suited for inclusion in ceasefire agreements (as opposed to other negotiating tracks of a peace process).

Table 1: Offensive cyber capabilities by goal of adversarial manipulation

Infrastructure Attack	**Data Attack**	**Denial of Service / Internet Shutdown**	**Information Extraction / Hack and Leak**
Examples: Stuxnet (2010); Ukraine (2015 and 2016); Iran and Israel (2020); India (2020)	*Examples:* Israel and Syria (2007); Shamoon 1.0 (2012) and 2.0 (2016); NotPetya (2017)	*Denial of Service:* Estonia (2007); Georgia (2009); *Internet Shutdown:* Syria (2011-present); Yemen (2018); Myanmar (2019).	*Examples:* Titan Rain (2003); Nagorno-Karabakh (2020)

2.1.1. Infrastructure Attacks

Sophisticated offensive cyber operations can directly attack strategic military and dual-use infrastructure in the opponent's territory to degrade their performance and even produce physical damage. The underlying intent of these types of offensive operations can shift across different phases of a conflict, for instance, from reconnaissance or small-scale operations through targeted disruption and sabotage attacks, to all-out systems-wide attacks on critical military and civilian infrastructure. The latter, for example, could theoretically attempt to paralyze energy, transportation, or telecom networks or even trigger explosions at hazardous sites such as nuclear power plants or oil and chemical plants (Shimeall, Williams & Dunlevy, 2001; Clarke & Knake, 2010). The software elements that undergird these advanced capabilities generally have two core components: a penetration component, which is the way by which the capability gains unauthorized access to a target network, and a payload component. If the payload is designed to cause damage to key installations, such as by causing machinery to malfunction, it could theoretically pose a threat to human lives, although to date this form of attack remains extremely rare (Lin, 2010; Lewis, 2011; Lindsay, 2013; Brantly, 2018).

The first and most well-known example of this type of capability to damage infrastructure emerged in 2010, when the US and Israel are widely believed to have sabotaged an Iranian nuclear enrichment facility using a computer worm that caused centrifuge industrial control systems to malfunction. This "Stuxnet" case is considered to be the first instance of a cyberattack known to have caused physical damage across international boundaries, though the ultimate effectiveness of the operation has been questioned (Lindsay, 2013). Ukraine also fell victim to this type of cyberattack on two separate occasions in 2015 and 2016, which temporarily took electricity networks offline by physically flipping circuit breakers in key substations (Zetter, 2016). Though the ultimate impact of this type of attack is also questionable (Maschmeyer, 2020), the 2015 attack represents the first known successful cyberattack on a country's electricity grid. In another recent high-profile case, Iran and Israel used offensive cyber capabilities to target control systems and cause some physical damage to each other's water treatment and port terminal facilities respectively (Melman, 2020). There is also speculation that cyberattacks could have been responsible for a string of explosions in Iranian nuclear facilities and a missile base during June and July 2020 (Sanger, Schmitt & Bergmann, 2020), as well as an electricity blackout in

Mumbai during fatal Sino-Indian border skirmishes in the same year (Sanger & Schmall, 2021).

In addition to the direct impact of this type of attack, a further impact, which is more difficult to evaluate, is the psychological effects of cyberattacks on sensitive national security infrastructure. In such a context, even if the attack produces limited physical damage, it could still alter strategic calculations about whether and how to pursue ceasefire negotiations.[1]

Aside from their potential stand-alone effects, these types of offensive cyber capabilities have a potential to play a role as enablers for wider conventional military operations. A potential example of this could be reports of a cyber subset of US war plans developed for use in a possible future conflict with Iran that would "unplug" Iran's cities, power grid, and military in the opening hours of a possible future battle (Schmitt & Barnes, 2019). The US reportedly had similar plans for the 2003 Iraq war and 2011 Libya intervention, but in both cases the US opted against deploying its capabilities due to uncertainty about the broader effects this might produce and the precedent it could set for other cyber powers to follow in future conflicts (Nakashima, 2011).

The use of offensive cyber operations to destroy or disable military networks, national infrastructure, or other types of computer systems may also occur in a civil war. Looking to the near future, it has been suggested that as the "Internet of Things" extends to vehicles and other tools employed by non-state armed groups, such as four-wheel vehicles and various types of drones, the potential will grow for governments fighting civil wars to conduct cyberattacks against the relevant computing components (Bronk & Anderson, 2017: 103–104). Examples of cyberattacks against infrastructure networks by non-state groups involved in civil conflicts are harder to come by, but not completely absent. In May 2019, Hamas's cyber command in Gaza reportedly attempted to undertake a cyber operation inside Israel. This apparently unsuccessful operation took place during a period of heavy exchange of rocket fire and air strikes between Hamas, Islamic Jihad, and the Israel Defense Forces. In response to the alleged cyberattack, Israel conducted an airstrike that destroyed the building housing the Hamas cyber capability (Chesney, 2019). Several years earlier, in 2015, the US claimed that the so-called Islamic State had launched cyberattacks on the US electricity grid. The US responded with an airstrike in Syria that killed Junaid Hussein, an

1 Authors' correspondence with Jakob Bund, January 2021.

Islamic State-affiliated computer hacker allegedly involved in the operation (Marks, 2015; Bronk & Anderson, 2017).

Some analysts predict that the low barriers of entry in terms of cost and expertise required to deploy basic cyber capabilities could facilitate new and expanded asymmetric conflicts, with small states and a range of non-state groups empowered to conduct cyber guerrilla campaigns against state infrastructure (Shimeall, Williams & Dunlevy, 2001; Liles, 2010; Lin, 2010; Tikk, Kadri & Liis, 2010; Maurer, 2018). There is already evidence that some states are utilizing non-state cyber proxies[2] to bolster their offensive cyber capabilities (Brantly, 2018; Maurer, 2018). For example, in May 2013, an Israeli official indicated that the Syrian Electronic Army, a group of hackers that supports the Syrian government, conducted a failed cyberattack against the city of Haifa's water infrastructure in response to an Israeli airstrike inside Syria (Ralph, 2013). It is also conceivable that these low barriers of entry could be exploited by hard-line factions within conflict parties to spoil the negotiations or the implementation of ceasefires that they disagree with.

However, significant infrastructure attacks also often require human-facilitated physical access to targeted networks and industrial control systems, while most non-state actors are typically limited to remote access (Maurer, 2018). For example, in the Stuxnet case, the attack relied on sophisticated code that likely required years of investing significant financial, software programming, technical engineering, and human intelligence resources to gain physical access to Iranian nuclear plant industrial control systems that had been hardened against cyberattacks by being deliberately disconnected from the global Internet. In addition, while these cyber operations can cause significant economic damage, and in some cases second-order impacts on human life (e.g., shutting off electricity), these impacts tend to be relatively short term, are often quickly resolvable, and must be combined with conventional military means to achieve significant results (Gartzke, 2013; Borghard & Lonergan, 2019). It might be that more advanced cyber capabilities to target critical infrastructure actually have high barriers to entry (Lindsay, 2013), and that only those states with the greatest conventional military power are likely to be able to effectively integrate them into combined terrestrial and cyber military campaigns.

2 Maurer (2018: xi) defines cyber proxies as "intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a [state] beneficiary."

In conclusion, despite the growing anecdotal evidence that cyber capabilities are being used to cause physical damage, there is still little research on how often this occurs, and what the significant effects may have been. The empirical research that does exist suggests that cyberattacks on infrastructure currently have only a limited direct impact on conflict (Borghard & Lonergan, 2019; Kostyuk & Zhukov, 2019; Maschmeyer, 2020). Such attacks tend to be very expensive, take time to develop, and produce uncertain effects (Gartzke, 2013; Lindsay, 2017; Kavanagh & Cornish, 2020; Maschmeyer, 2020). Furthermore, even in the worst of scenarios, the costs to human life are limited compared to even very minor kinetic attacks that routinely occur during conflict (Maurer, 2011; Borghard & Lonergan, 2019). They also seem to be relatively divorced from events on the battlefield (Kostyuk & Zhukov, 2019).

2.1.2. Data/File Damage

An alternative class of offensive cyber capabilities seeks not to produce physical damage, but instead undermine the confidentiality, integrity, or availability of data contained on computing systems. These attacks also generally require that computer or network systems be penetrated, after which destructive code is run on an individual machine or is inserted on a broader server to which the machine is connected (Bellovin, Landau & Lin, 2017). In this case however, the main target of the payload component is data stored on the machine or network rather than exploiting industrial control systems to cause physical damage. In Ukraine in 2017, for example, the NotPetya destructive malware spread through commonly used tax software. The attack, which has been linked to pro-Russian hackers operating amidst the ongoing armed conflict in eastern Ukraine, disabled an estimated 500,000 computers in Ukraine alone, and spread across 65 other countries, causing widespread problems in the public and private sector (Maschmeyer, 2020). The "resulting economic disruption shaved an estimated 0.5 percent off Ukraine's GDP in 2017" (Maschmeyer, 2020). While it was largely disconnected from the situation on the battlefield, the consequences for the economy potentially impacted the balance of power in the conflict (Maschmeyer, 2020). This form of data attack can be very disorienting and impactful, especially when occurring in the midst of an armed conflict (Bellovin, Landau & Lin, 2017).

There are cases of this type of cyber capability also reportedly being utilized on the battlefield. For example, Israel reportedly used cyber means to spoof Syrian early warning radars during an air raid that destroyed an alleged

Syrian nuclear facility in 2007. This cyber capability is said to allow users to invade communications networks and replace sensor data with a "false sky" or manipulate sensors into positions where approaching aircraft cannot be seen (Fulghum & Barrie, 2007). These types of cyber operations have reportedly also been used by the US in Iraq and Afghanistan to disrupt insurgents' communications networks. In Afghanistan, for example, a US general publicly reported using cyber operations to get inside and "infect" Taliban command and control networks to "great impact." (Satter, 2012).

Yet while attacks on data and computers can be significant, as seen with the wider implications of NotPetya in Ukraine, there is also a notable risk of collateral damage, as indirect dependencies are hard to identify.[3] For example, an attack on the systems of a foreign or defense ministry might well spread to the health sector within the same country or an organization using a similar system internationally. These unexpected consequences could limit the usefulness of the capabilities; for example, it seems to have been exactly these concerns that prevented the US from deploying cyber capabilities at the onset of the Iraq war and the Libya intervention.

2.1.3. Denial of Service / Internet Shutdowns

Physical infrastructure- and data-centered cyberattacks on an adversary's networks require some type of unauthorized access. In contrast, another common, if crude, form of offensive cyber operation that does not require unauthorized access is a Distributed Denial-of-Service (DDoS) attack. This entails flooding an adversary's networks with incoming traffic from many different sources to overload and potentially take the network offline. DDoS attacks can and have been weaponized in a conflict context. For example, in Georgia in 2008, a DDoS attack coincided with a Russian military intervention and temporarily took the government's websites and official communications systems offline. By obstructing the flow of military and intra-governmental information, this attack made it more difficult for the Georgian authorities to organize a coherent response to the crisis and limited the ability of the president to inform citizens of important updates (Hart, 2008; Markoff, 2008; Hollis, 2011). This was the first clear case of a coordinated cyberspace domain attack synchronized with major combat operations (Hollis, 2011), and it "played a significant, if not decisive, role in the conflict"

3 The NotPetya attacks demonstrate the potential for wider collateral damage, though in this case the wider damages were very likely a desired effect.

(Deibert, Rohozinski & Crete-Nishihata, 2012: 3). In another example, albeit not part of an armed conflict, a DDoS attack in 2007 succeeded in temporarily shutting down Estonia's digital infrastructure and cutting the country off from the global Internet (Landler & Markoff, 2007) – a capability with obvious strategic utility if deployed in conjunction with a conventional military offensive and/or other cyberattacks. Some state actors are presently alleged to maintain "botnet armies"[4] that can be activated to conduct disruptive DDoS attacks in peacetime or support conventional military operations in an armed conflict.[5]

A different type of denial-of-service attack entails actors utilizing their "higher-level" capabilities or existing control of networks to manipulate systems in their strategic interest. An important example during intra-state conflicts is the implementation of localized internet shutdowns. We recognize that such actions are not typically included under the umbrella of offensive cyber capabilities. However, we include them here as they have a similar goal to other denial-of-service attacks, that is, to deny an adversary access to a network that is important to their internal communications or military operations. The fast-growing use of internet shutdowns by governments around the world in response to various forms domestic unrest[6] also suggests to us that shutdowns could become an increasingly important tactic in civil wars. This is significant because these intra-state wars are the predominant form of contemporary armed conflict and thus the most frequent subject of ceasefires.

Internet shutdowns are generally undertaken by governments who have control over the state infrastructure and seek to block armed opposition groups' use of internet-enabled systems for military purposes. In this context, cyber capabilities are used to support, and potentially enhance, conventional operations. Gohdes (2015: 355) has shown that competent non-state groups benefit extensively from cheap encrypted communications tools which serve as their secure military communications networks and geographic information systems applications to accurately locate military targets and calibrate indirect fire weapons such as mortars and rockets. This creates incentives for

4 Botnet armies are networks of computers infected by malware to enable their remote control by single actor, for example a national military or intelligence service.

5 For example, North Korea. See Jun et al. (2015).

6 One NGO documented 213 total internet shutdowns in 33 countries in 2019 that were implemented by governments in response to events such as protests, communal violence, and elections, almost three times the 75 shutdowns documented in 2016 (Taye, 2018, 2020).

governments to undermine this technology by shutting down the Internet in strategic periods or locations, in particular when launching conventional military offensives. Gohdes (2015: 356) finds evidence for this in a study of localized internet shutdowns during the Syrian civil war. The analogous nature of this tactic to the use of DDoS attacks to disrupt official Georgian communications in conjunction with a major conventional military operation in 2008 should be apparent.

The implementation of internet shutdowns for this purpose does not appear to be limited to Syria. In Myanmar, news outlets reported that there were internet shutdowns in ethnic states during large combat operations by the national military (Beech & Nang, 2019; Radio Free Asia, 2019) and following the military coup in early 2021 (Tønnesson, 2021). Similarly, in India, local internet shutdowns are reported to take place amidst "military actions by armed forces or paramilitary units" (Taye, 2020: 20). Interestingly from the perspective of ceasefire design, Gohdes (2015) suggests that non-state groups could come to use internet shutdowns as an early warning system of conventional military attacks.

The civil wars in Yemen and Libya have even featured internet shutdowns carried out by non-state groups. In Yemen, the non-state Houthi movement's physical capture of telecom operators' headquarters in the capital of Sana'a have reportedly allowed it to slow down or disable the Internet in conflict zones such as Taiz and to block internet domains that report on its troop movements (INSIKT Group, 2018; Coombs, 2020). In Libya, meanwhile, armed protestors occupied the headquarters of the state-owned internet provider and temporarily forced it to switch off internet services for large parts of the country to leverage political demands (Al Jazeera, 2013).

2.1.4. Information Extraction

Modern espionage relies heavily on signals intelligence (i.e., intercepting telecoms and internet-based communications) (Shires, 2020). These activities are undertaken mainly by intelligence services, but might also involve "hacktivist" proxies and others. With regards to offensive cyber capabilities, information extraction operations are understood as distinct from cyber reconnaissance of an adversary's networks to prepare the ground for potential future infrastructure attacks. Rather, the goal is gathering information for future political or military ends. For example, in the lead up to and during the outbreak of armed conflict in Nagorno-Karabakh during late 2020, Armenian hackers allegedly broke into Azerbaijan's government websites and

released personal information of Azerbaijani soldiers and purported Azerbaijani government email correspondence (Thomas & Zhang, 2020).

This type of espionage can, however, have a very real impact when deployed for repressive purposes (Deibert, 2015; Rød & Weidmann, 2015; Keremoğlu & Weidmann, 2020). Offensive cyber capabilities can provide an efficient means to uncover evidence against political opponents to support extrajudicial killings, arbitrary detention, and other forms of state repression (King, Pan & Roberts, 2013; Gunitsky, 2015). There is now significant empirical evidence detailing the use of digital surveillance technologies by authoritarian regimes against their opponents (Anceschi, 2015; Deibert, 2015). While this use of offensive cyber capabilities is less likely to have a direct impact on battlefield violence, it provides a complementary tool to support state violence.[7]

Indeed, information gathered through espionage is often strategically released in so-called "hack and leak" operations. This combines "intrusion into networks with coordinated and doctored dissemination through traditional and social media" (Shires, 2020). Such approaches can be an effective way to damage an adversary or manipulate public opinion against political or military opponents. In many cases, these methods are a "'simulation of scandal' – deliberate attempts to direct moral judgement against their target" (Shires, 2020). While this use of offensive cyber capabilities is not necessarily linked to battlefield violence, it could provide a complementary tool to support military campaigns. There is also a propensity for such operations in the grey zone between peace and conflict (Harknett & Smeets, 2020; Shires, 2020).

Ultimately, we are not persuaded that ceasefire negotiations are the best forum to manage this category of cyber capabilities. As explained, ceasefire agreements focus on stopping armed hostilities. Addressing the serious consequences of hack and leak operations may be increasingly important to sustainable conflict resolution. However, it is perhaps better addressed in other tracks of peace negotiations. Indeed, to date, only a handful of peace processes have made basic attempts to regulate the parties' use of social media to incite violence or spread disinformation, with the October 2020 Libya

7 Beyond the state as cyber capabilities lower the threshold for extraterritorial actions (e.g. digital surveillance of the contacts of Saudi dissident Jamal Khashoggi appear to have played a role in his assassination).

ceasefire agreement being the most detailed case so far.[8] And where these provisions do appear, they are just as likely feature in codes of conduct, national dialogue outcomes, and electoral agreements as opposed to the text of ceasefire provisions.[9] Even in the Libya ceasefire noted above, issues of hate speech and incitement are also being addressed in the political track of ongoing peace negotiations.[10] We have included information extraction operations here for the sake of completeness. However, we devote limited attention to how this category might be incorporated into ceasefires in the following discussion.

8 This ceasefire agreement refers to possible judicial action against websites and TV channels broadcasting hate speech, possible communication with social media companies to remove offending content, and the establishment of a follow-up sub-committee. See Section II, Article 5 of the 23 October 2020 "Agreement for a Complete and Permanent Ceasefire in Libya," full text available at unsmil.unmissions.org/sites/default/files/ceasefire_agreement_between_libyan_parties_english.pdf.

9 For relevant examples, see the 2015 Samburu and Turkana Ceasefire Agreement in Kenya, 2017 South Sudan Cessation of Hostilities Agreement, 2018 Tripoli Ceasefire Agreement in Libya, 2020 Agreement for a Complete and Permanent Ceasefire in Libya, 2008 Sotik and Borabu Districts Social Contract in Kenya, 2014 Code of Conduct for Political Parties and Candidates in Myanmar, 2017 Agreement to Promote National Dialogue in Yei River State and South Sudan, and 2020 Code of Conduct for the Libyan Political Dialogue Forum (agreement texts available at peaceagreements.org or on file with the authors).

10 Article 3 of the Libyan Political Dialogue Forum code of conduct includes principles related to rejecting hate speech and incitement to violence.

3. Ceasefires

3.1. What Is a Ceasefire?

Ceasefires are arrangements that seek to stop violence related to armed conflict. Unlike peace agreements, ceasefires do *not* resolve the conflict by addressing its broader political or socio-economic causes. As stressed in the forthcoming UN Ceasefire Guidance, beyond the commitment to stop armed violence, there is notable variation in what a ceasefire includes. To account for this reality, we distinguish three classes of agreement: "Cessation of Hostilities (CoH)," "preliminary ceasefires," and "definitive ceasefires." (For more information see, Brickhill, 2018; Clayton et al., 2019; Hottinger, 2019; Clayton & Sticher, 2021; United Nations, forthcoming):[11]

CoH are informal, temporary arrangements that suspend fighting, but lack any significant provisions to monitor or verify compliance. They can come in a variety of forms, from unilateral to bi/multi-lateral, and may not even be written down. Despite their relatively informal character, CoH are often important because they can represent the first real step by the conflict parties towards negotiation and ending violence (Brickhill, 2018).

Preliminary ceasefires, by contrast, are always formal ceasefire agreements. Practitioners and security experts tend to reserve the term ceasefire for this more formal bi/multi-lateral agreement that involves some form of disengagement and monitoring and/or verification (Brickhill, 2018: 40–41). Preliminary ceasefires specifically link to and often aim to further a broader peace process aimed at resolving the political disputes underlying the conflict. They are typically put in place after a period of substantive negotiations.

Definitive ceasefires are the most comprehensive type of ceasefire and arise at the end of the peace process. Importantly, they also include provisions to disarm and demobilize the conflict parties and to institutionalize security cooperation. Unlike other ceasefires, which seek only to suspend the fighting, definitive agreements aim to terminate armed conflict. Definitive ceasefires are therefore a key outcome of peace talks, entering into effect alongside a peace agreement addressing the political issues of dispute (see, Clayton et al. 2019).

11 In practice, the delineation between these terms (and between cessations and preliminary ceasefires in particular) may not always be completely clear cut. Nonetheless, the use of these terms is helpful in analyzing the form and objective of different types of agreements.

3.2. What Are the Functions of a Ceasefire?

Supporting the Negotiation Process: As a peace process develops, ongoing hostilities can become prohibitive to progress in negotiations. In such cases, ceasefires can help to "de-link" the negotiation process from the battlefield. If this does not happen, violence can eventually undermine talks and lead to their collapse. Ceasefires can then help to create a context more favorable for dialogue (Clayton & Sticher, 2021).

Enabling Humanitarian Assistance: Ceasefires can of course also occur for more limited purposes not strictly linked to the political process (Clayton, Nathan & Wiehler, 2021). This often involves temporal or geographically limited ceasefires to facilitate the provision of humanitarian assistance to war-affected populations.

Demonstrating Command and Control: Complying with a CoH or preliminary ceasefire demonstrates some level of command and control over an armed force (Smith, 1995). This form of signaling can be a necessary precondition for advancing a peace process, in particular when actors doubt their opponent's ability to implement future settlements. For example, when a conflict involves a fractured opposition or widespread use of irregular or proxy forces (an anticipated problem with hacker groups and other proxies in the context of cyber operations), it might be necessary for an actor to first demonstrate control over their armed force before their opponent is willing to engage in broader peace talks.

Imposing Costs: Formal ceasefires can also put into place certain structures that create reputational and other costs for any conflict party that violates their terms. Ceasefire agreements serve as a benchmark against which powerful international actors can evaluate ceasefire signatories' behavior. Reneging on a ceasefire agreement thus generates what are referred to in the academic literature as "audience costs" (Fortna, 2003: 343) that would not have occurred in the absence of the ceasefire deal. In this sense, signing a ceasefire agreement is never "cheap talk," i.e., "costless, nonbinding, unverifiable messages" (Farrell & Rabin, 1996: 116).

Seeking Tactical Advantage: The costs a belligerent suffers when reneging on a ceasefire can sometimes be outweighed by the tactical advantages gained from a return to violence. Suspending hostilities can allow belligerents to rearm and recruit new members, as well as temporarily reduce the costs of military conflict. Belligerents can therefore enter into a ceasefire for tactical military reasons, and then return to violence having

secured the benefits sought from the fighting break (Clayton, Nathan & Wiehler, 2021).

Signaling Intentions: As the foregoing suggests, it is never fully clear whether an actor is genuinely interested in advancing the political negotiation process, using ceasefire talks to improve their military position or score political points, or somewhere in between (Chounet-Cambas, 2011: 7–8, 20; Crocker, Hampson, & Aall, 2004: 158; Gartner & Melin, 2009: 566; Toft, 2010: 15). Given that actors may have an incentive to misrepresent their specific objectives, simply announcing one's peaceful intentions is unlikely to be sufficient to convince the other side to agree a ceasefire that risks benefitting their opponent. Instead, actors often need to send a signal that imposes some cost on themselves to demonstrate a commitment to peace (Morrow, 1999: 484).

In this respect, ceasefire agreements offer belligerents a tool through which to exchange information about their (hard to observe) intentions. By entering into, abiding by, or reneging on an agreement, belligerents can communicate some set of preferences while also assessing the intentions and abilities of their opponent (Werner & Yuen, 2005). Honoring the terms of a ceasefire communicates the will and capacity to uphold agreements. In this way, a CoH or preliminary ceasefire can be a useful confidence building measure to demonstrate some level of good faith intention, signaling (to a lesser or greater extent) a desire to move tentatively towards peace while also allowing belligerents to keep their fighting capability intact.

3.3. What Is Included within a Ceasefire Agreement?

Every ceasefire agreement is unique and (ideally) designed to reflect the specific characteristics of the conflict to which it relates. However, there are also some common features that we observe across ceasefire agreements.

By definition, a ceasefire agreement will always include some commitment to stop hostilities. However, there is notable variation in the scale and scope of activities that the parties prohibit and the detail in which this is agreed. Common inclusions are military attacks, acquiring equipment, training or recruiting troops, redeploying forces, terrorism, and sexual violence.

Ceasefires tend to be more effective when they are precise regarding what behaviors are prohibited (Haysom & Hottinger, 2004; Potter, 2004; Brickhill, 2018). Agreements that seek to produce a durable suspension of

violence should ideally go into considerable depth, mapping out and defining the obligations on the parties and being clear on the specific sanctions associated with any violations (Potter, 2004). Precision and clarity in the agreement makes it easier for the parties to abide by it and determine when it has been breached (PILPG, 2013). Conventional ceasefires therefore typically include provisions to establish the specific time and date when the included obligations begin and the precise geographic scope of the areas to which they apply. In contrast to vague commitments to cease hostilities, which fail to map out the actors, timelines, and responsibilities, well-defined prohibitions make successful ceasefire implementation more likely.

Belligerents engaged in armed conflict are unlikely to trust each other to abide by the terms of any agreement. In this context, ceasefire management mechanisms along with associated monitoring and verification activities can help to increase the predictability and sustainability of a ceasefire (Buchanan, Clayton & Ramsbotham, 2021). Ceasefires are often designed then with the expectation that they will almost inevitably be violated but that this does not necessarily need to result in the failure of the agreement. Rather, they aim to foster a problem-solving working method whereby the parties will jointly develop solutions to challenges encountered during ceasefire implementation and to prevent their repetition.

Ceasefire agreements can therefore include provisions to create new bodies that manage and support the implementation of a ceasefire. The functions and composition of ceasefire management bodies can take a range of forms, including joint commissions or liaison structures between the conflict parties (Brickhill, 2018). Stein (2019) underscores the overall importance of these institutions to the robustness of ceasefire implementation, given that in such bodies the conflict parties must work together daily to manage the ceasefire.

Within the overall ceasefire management structure, some ceasefire agreements also include a mechanism to monitor and verify the terms of an agreement and serve as an early warning mechanism, allowing the parties to determine if the process is on track (Brickhill, 2018: 49). These monitoring provisions often receive significant attention during ceasefire negotiations and provide for some actor (domestic, international, or a combination of both, often in collaboration with the conflict parties) to monitor the agreement signatories and ensure they are complying with the terms of a ceasefire, completing any predefined tasks, and addressing problems as they arise (Fortna, 2004; Haysom & Hottinger, 2004; United Nations, forthcoming). In this way,

agreeing to these provisions means that the actors voluntarily take on additional self-imposed costs in the event that they renege on a deal. Thus, accepting monitoring arrangements can signal a stronger intention to abide by the agreement. Monitoring activities are also intended to prevent the escalation of either genuine accidents or low-level violations that might otherwise escalate into full-blown conflict. Monitoring and verification provisions are therefore associated with more durable and successful ceasefires in both intra- (Clayton & Sticher, 2021) and inter-state conflict (Fortna, 2003).

3.4. Rationales for Including Restraints on Offensive Cyber Capabilities in Ceasefires

Having set out the types, purposes, and contents of a ceasefire, we turn to the question of how and whether restraints on offensive cyber capabilities should be included in a ceasefire agreement (as opposed to, for example, being a separate standalone part of the conflict management and resolution process). In answering this question, we acknowledge the qualitative differences between cyber and conventional military operations. Notwithstanding this, there are three main reasons to consider cyber capabilities when constructing a ceasefire: an increased military use of cyber capabilities in armed conflict, the risk that unrestrained cyber operations could pose to the stability of a broader ceasefire regime, and signaling and confidence building.

The primary purpose of ceasefires is to control and stop violence. We therefore believe that if cyber capabilities have been utilized in a conflict, the first two rationales argue especially strongly in favor of incorporating cyber restraints into conventional ceasefires. If, on the other hand, the objective of the conflict parties in negotiating restraints on offensive cyber operations is purely limited to signaling, confidence building, or creating space for political negotiations, we would not wish to rule out the possibility of a standalone cyber de-escalation agreement. As always, rather than blind conformity to any pre-set approach, the specific characteristics of the conflict and interests and needs of the parties should be the paramount factor in choosing the format by which to negotiate any conflict issue. We now provide a fuller explanation of the three main rationales for including restraints on cyber capabilities in ceasefires.

Increasing Convergence of Military and Cyber Capabilities: As of early 2021, there is a small but growing set of cases where cyber capabilities have been deployed as a tool in armed conflict to produce real-world damage. This involves the direct targeting of civilian (e.g., India, Iran, Israel, and Ukraine) and military/intelligence infrastructure (e.g., Iran).[12] The use of cyber capabilities therefore have the potential to result in injury and loss of life. While the deployment of such capabilities is at present limited to a small number of cases, it is becoming more common and has the potential to cause physical violence that would ordinarily be regulated within a ceasefire agreement.

In addition, there is a larger collection of growing cases in which cyber operations are used as support weapons to shape events on the battlefield by disrupting an opponent's military and government network services and data as part of a wider military campaign. This most often revolves around coordinated military and cyber operations, including data attacks, denial of service, and internet shutdowns. In these cases, the use of offensive cyber capabilities does not in and of itself represent violent behavior but rather supplements the broader war fighting effort. A possible analogy is troop movements in a conventional ceasefire arrangement. While troop movements do not alone present a direct threat to an opponent, the strategic advantage gained through such maneuvers might sufficiently threaten an opponent that they opt to escalate and respond militarily. For that reason, troop movements are often tightly regulated in a ceasefire.

One critique which could be levied at this argument is that in principle, any activities with the potential to cause physical violence or produce military advantage should be covered within a general ceasefire, even if all of the precise instruments of violence remain unnamed. So, if the parties commit to stopping violence, this could also reasonably be assumed to cover behavior in cyberspace. However, as we discuss above, one of the consistent themes emerging from practitioner accounts of ceasefires is the need for precision around prohibited behavior. Creative ambiguity can at times be useful when seeking political consensus in a broader peace agreement, but it is not appropriate in ceasefires where the lack of precision represents a major risk to successful implementation (Haysom & Hottinger, 2004). Thus, clearly setting out the prohibition of this increasingly common technology is likely to be more effective.

12 In June 2019, US Cyber Command said it had conducted online attacks against an Iranian intelligence group in response to what US officials claimed was the role it played in planning attacks that used mines to disable two oil tankers in the Persian Gulf (Barnes & Gibbons-Neff, 2019).

Risks of Cyberattacks Undermining a Broader Ceasefire Regime: A successful ceasefire requires that the parties have a common understanding of their commitments (Potter, 2004; Brickhill, 2007, 2018; PILPG, 2013). If the cyber dimension is excluded from ceasefire negotiations, there is a risk of confusion that might undermine the broader ceasefire arrangement. Cyber activities are especially likely to produce significant confusion in this regard given their relative newness and the broad international disagreement on how to understand and regulate these capabilities. Conflict parties are then more likely to perceive offensive cyber operations quite differently and thus respond unexpectedly or in a cross-domain fashion that could pose a risk to the stability of a broader ceasefire. The growing permeability between cyber and conventional military operations, with conventional military attacks producing a cyber response (e.g., US-Iran) and cyberattacks leading to a conventional response (e.g., Israel-Hamas), indicates the risk that cyber-related incidents might pose for a conventional ceasefire. Moreover, hard to predict dynamics create a significant threat of escalation, as differences in "strategic and organizational culture, regime type, strategy and doctrine, and force deployment may mean that what is perceived as a relatively low-cost cyber response by one state may be in fact cross a key threshold of the other." (Borghard & Lonergan, 2019).

This is less likely to be the case if a ceasefire process addresses this cybersecurity dilemma by being as specific as possible with regards to any potentially ambiguous actor, topic, or commitment related to different cyber capabilities. The inclusion of definitions within the ceasefire agreement on terms such as cyber operations and attacks as well as critical or national infrastructure may likely also be useful for the practical purpose of implementing the agreement and may be warranted to ensure the desired common understanding between the signatories.

Signaling and Confidence Building. As described, one key function of ceasefires is to send signals regarding a desire to negotiate in an environment of mistrust and hard to read intentions. However, the peaceful signal intended to be sent through a ceasefire could be undermined if offensive cyber operations were to continue during the ceasefire period. In contrast, if the signatories recognize in a ceasefire agreement that offensive cyber operations are potentially a threat to the peace, and they commit to cease and desist such hostile activities, this is in and of itself potentially an important signal to an opponent of a greater openness to restricting all forms of violent behavior

and pursuing political negotiations (assuming such operations were prevalent in the past).

Within the overall rubric of signaling and confidence building, there may also be a strong humanitarian rationale for including restraints on offensive cyber capabilities in a ceasefire. In particular, even offensive cyber operations directed against military targets can have unforeseen and unintended effects on the civilian population as a whole. This is due to the potential for network outages to produce cascading effects or the unexpected propagation and spread of malicious code used in the operation (Bellovin, Landau & Lin, 2017). Notably, US war planners chose not to deploy cyber capabilities in military campaigns in Iraq in 2003 and in Libya in 2011 due to concerns that the effects of the cyber operation would spread beyond the air defense systems that were to be targeted. As cyber capabilities become a more common part of military campaigns, the inclusion of restraints on cyber activities within a ceasefire agreement might therefore also become a humanitarian confidence building measure intended to limit potential harm to civilians.

3.5. Challenges to Incorporating Restraints on Offensive Cyber Capabilities in Ceasefires

Despite multiple rationales for incorporating offensive cyber capabilities into a ceasefire, there are significant complications entailed with this task. We set out five main challenges.

Monitoring, Verification, and Attribution: The monitoring and verification of offensive cyber operations is notoriously difficult. Attribution is a problem for conventional ceasefires, as determining if, when, or which conflict party violated the terms of an agreement is challenging even in the physical world. Yet conventional weaponry leaves much bigger clues and can be investigated via established means (Verjee, 2019). This is not the case for cyber activities. In cyberspace, there are an unknown number of state and non-state actors who possess offensive cyber capabilities and millions of (largely unsuccessful) cyberattacks of different degrees of gravity and intensity every second.[13]

13 Nye (2017) states that the US Defense Department faces ten million intrusion attempts into its networks per day.

It is thus generally difficult to identify the actors involved in any given cyber-attack, the source of the incident, and the extent to which any actors operated independently, making the monitoring of the prospective cyber components of a ceasefire especially challenging.[14]

Notwithstanding this, attribution is not impossible. The technical capacities to attribute attacks are increasing both among governments and private cybersecurity companies (Rid & Buchanan, 2015; Nye, 2017; Maurer, 2018). As discussed, there is a relatively limited number of actors with the resources to produce the most sophisticated infrastructure attacks, meaning it is often relatively clear who was responsible for certain activities. In these cases, attribution can become a (significant) political rather than technical problem. Intelligence collection and political analysis can also bolster technical conclusions (Lewis, 2011; Healey, 2012b; Rid & Buchanan, 2015). Furthermore, it is worth recalling that even in conventional ceasefires, monitoring and verification is not a "all or nothing" proposition. Rather, monitoring and verification arrangements vary substantially in scope, detail, and mandate from information sharing and reporting all the way to verification, accountability, and sanctioning violations (United Nations, forthcoming).

So, while some forms of attribution are possible, technical limitations mean some conventional monitoring – and especially incident verification and attribution modalities – are unlikely to be feasible for cyber provisions of a broader ceasefire agreement. This will require major conceptual re-thinking of a tool currently widely viewed as essential to successful ceasefire implementation. In this respect, it is important to recall that even in conventional ceasefire monitoring, attribution is not an end in and of itself but rather one means to support joint problem-solving, to prevent recurrence, and, ultimately, to promote the desired policy outcome of a stable ceasefire regime.

Balancing Precision and Implementability: As we note above, it is widely agreed that specific and precise ceasefire agreements tend to be more effective. Cyber capabilities make it very challenging to be precise; they are unpredictable, uncharted, constantly evolving, and can be initiated by many different types of actors. Parties might agree to limit certain capabilities, but the diversity across capabilities might make implementation challenging.

14 Determining who has responsibility for malicious cyber activity can be understood in a variety of ways. Attribution can relate to determining the machine or location from which the malicious cyber activity occurred, the specific perpetrator(s) involved, or to an adversary who is ultimately responsible for the operation (Lin, 2016).

Moreover, "overpacking" ceasefire agreements with a plethora of potentially unimplementable provisions risks distracting attention from more pressing sources of violence, overwhelming the conflict parties, and, ultimately, undermining a process. To this end, the benefits of incorporating cyber provisions within a ceasefire must always be weighed against the potential limitations. Furthermore, the relative benefits of managing cyber dimensions within the ceasefire process *vis-à-vis* alternative theatres of negotiation (e.g., broader peace negotiations, regional or global systems of governance) should be considered.

Broadening Participation: Incorporating offensive cyber capabilities into ceasefires requires the participation of a number of additional actors that risk complicating the negotiation process. The creation of implementable conventional ceasefires requires input from the military leaders who have sufficient understanding of the context on the battlefield and what is (and is not) feasible militarily. In many cases, these conventional military figures will not have sufficient technical expertise to negotiate and implement provisions regulating cyber activities.

As such, ceasefire negotiations are likely to require technical experts from the conflict parties that hold sufficient knowledge of how offensive cyber capabilities work. Indeed, including relevant technical expertise from both sides into ceasefires has in general been shown to make it more likely that any ceasefire implementation and monitoring efforts have a realistic mandate and sufficient funding, personnel, and equipment (Potter, 2004). The negotiation of any cyber components of ceasefires could necessitate the involvement of military cyber commands, intelligence agencies engaged in offensive cyber operations, or national Computer Emergency Response Teams (CERT) / Computer Security Incident Response Teams (CSIRT).[15] Introducing these new actors and technical components, however, risks complicating the negotiation process and hampering likely urgent efforts to find an agreement to limit kinetic military activities. There is also likely to be notable asymmetries in the technical capabilities of the parties, which might further reduce vital trust in the process. Finally, some of the relevant actors and intelligence agencies might be unwilling to acknowledge their activities or formally attend the talks.

15 CERTs/CSIRTs are groups of experts that assesses, document, and respond to cyber incidents so that their organization or jurisdiction's network(s) can recover and avoid future incidents.

Beyond the make-up of the conflict parties' delegations, it must also be borne in mind that cyberspace is a global domain consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, and computer systems (von Heinegg, 2012: 9–10). The private sector own up to 80–90 per cent of this infrastructure (Lewis, 2011; Lindsay, 2013; Hartmann & Giles, 2018), which means that private entities often have some control over the ease of movement of data and code involved in cyber operations (Hare, 2009; Lewis, 2011) and could also need to be persuaded to participate in ceasefire talks and implementation planning. Prospective outside involvement in the process could further include companies that develop the software packages used to conduct cyber operations, cyber incident responders, and academic and research institutes that have the expertise to investigate cyber incidents. A heretofore unknown role for the private sector and other outside technical actors in ceasefire negotiations would certainly require extensive thought, although it could be considered to fall within the rubric of what UN draft Ceasefire Guidance refers to as civilian ceasefire monitoring (United Nations, forthcoming).

Non-Physical Nature of Cyberspace: Complicating matters further is that offensive cyber capabilities reduce the barrier that physical geography poses to conflict (Gartzke, 2013). Specifically, offensive cyber operations can sometimes traverse third-party networks and neutral states to reach their intended target (Geers, 2011; Lewis, 2011). For example, when the Estonian Internet came under a virtual blockade through a DDoS attack in 2007, malicious traffic simultaneously entered Estonia from some 130 to 180 countries (Tikk, Kadri & Liis, 2010; Healey, 2012a). More advanced cyber operations can also make use of computers and servers in third-countries when infiltrating targeted networks. For example, a 2013 cyberattack in South Korea that damaged 32,000 computers and the network availability of six media and financial companies was suspected by Seoul to have been carried out by North Korea, despite the attackers having used Chinese Internet Protocol addresses when implanting the malicious code (BBC News, 2013).

Neutral states can thus be witting or unwitting facilitators of malicious traffic and could be requested under a prospective ceasefire to take some responsibility for the traffic passing through or botnets being hosted on their territory (Healey, 2012a; von Heinegg, 2012). Likewise, "hactivist" groups, state cyber militias, proxies, and contractors, (Liles, 2010; Hare, 2012; Lin, 2012; Brantly, 2018; Weber, 2018) can all take action to disrupt or

damage an opponent's data, networks, and infrastructure from a formally neutral state's territory, with varying levels of inspiration, tolerance, and even direction from the relevant government (Tikk, Kadri & Liis, 2010; Maurer, 2018). The non-physical nature of cyberspace thus poses a new and distinct challenge for ceasefire agreements in terms of a potential need to obtain commitments from third-party or neutral states with respect to malicious actions taking place or transiting their territory.

Delineating Espionage and Military Operations: It is challenging to distinguish offensive cyber capabilities intended to cause direct disruption and damage to data, networks, and infrastructure from the broader range of cyberespionage tools. Both cyberattacks and cyberespionage operations need to first gain access to a computer system before they can achieve an effect (except for DDoS attacks). Furthermore, intelligence agencies (rather than national militaries) have been central to the conduct of both forms of cyber operations (Maurer, 2018; Kavanagh & Cornish, 2020). Consequently, cyberespionage activities and steps to "prepare the battlefield" for future cyber infrastructure or data attacks by obtaining unauthorized accessed to opponents' networks can "look identical from the victim's perspective, with sophisticated technical analysis and wider threat characteristics required to distinguish between the two" (also see, Buchanan, 2017; Egloff & Shires, 2020). This poses problems for ceasefires, as it is unclear if any unauthorized access to a network is preparation for an attack or espionage. For example, if an actor gains access to a system to create a backdoor but without triggering an effect, is this prohibited? Or should early activity such as preparing the battlefield be prohibited as well? These are difficult technical questions that could need to be addressed by a ceasefire process.

4. Questions and Options for Peacemakers

There can be no one-size-fits-all model for the incorporation of restraints on offensive cyber capabilities into ceasefire processes. However, there are several possible approaches that could be tailored to a conflict. Building on this logic, we structure our discussion around three key sets of questions for peacemakers to consider:

1. In a given conflict setting, what are the conflict analysis pre-requisites for determining whether cyber capabilities should in fact be included in ceasefire negotiations?

2. What negotiation process design choices could help to enable discussion on cyber capabilities, including the structure of talks and participation decisions?

3. What could specific prohibitions, commitments, and management and coordination mechanisms on offensive cyber capabilities look like? Practically speaking, how would they fit together in a ceasefire agreement?

In considering these questions, we address some of the challenges related to incorporating offensive cyber capabilities into ceasefires which were identified in the preceding section. Namely, difficulties in monitoring and verifying cyber incidents, balancing precision with implementability, integrating new classes of participants into ceasefire talks, the non-physical nature of cyberspace, and how to handle cyberespionage.

Proposing templates and guidance for negotiations is potentially problematic, but this can also be useful as a guide to complex processes, which "help focus our thinking and provide a basis for strategic planning" (Brickhill, 2018; 47). Given that cyber operations remain a relatively new part of warfare – and that this is the first attempt (we know of) to explore its influence on the ceasefire process – the proposals here should be considered to be the starting point rather than the final word on the subject or a fixed set of instructions to be mechanically followed.

4.1. Preparing for Talks on Offensive Cyber Capabilities

Obviously, in cases in which offensive cyber capacities have played no significant role in the conflict, there is no reason to take this further as part of ceasefire negotiations. Indeed, the last thing we would want is to unnecessarily complicate the already challenging task of agreeing a ceasefire by adding irrelevant issues to the agenda. However, we believe that cyber capabilities should now be part of any initial conflict analysis. If such research reveals cyber components to be part of the conflict context, it is then important to raise the issue with the conflict parties for consideration of whether and how to design the ceasefire process to incorporate this issue.

4.1.1. Cyber Conflict Analysis

At the outset of negotiations, peacemakers should determine the extent to which offensive cyber capabilities have been used during the conflict. In some cases, offensive cyber capabilities may have been publicly deployed (e.g., Ukraine), while in other cases, their use might not be widely known or documented. To assess if offensive cyber capabilities have been used as part of hostilities, proactive research, outreach, and coordination efforts are likely to be required. This is in line with the recommendation of the UN's Report on Digital Technologies and Mediation for mediators to consider the "digital ecosystem" in their conflict analysis.[16]

Such an assessment could be incorporated as part of a conflict analysis aimed at developing process design options for the forthcoming mediation (e.g., as part of an Actors, Content, Context, Process (ACCP) Conflict Exercise[17]), and it is likely to include taking advice from the conflict parties and their communities. Some key questions might include:[18]

- Has any party to the conflict stated that they would use offensive cyber capabilities/operations in response to or to prevent an attack?

16 See: peacemaker.un.org/digitaltoolkit.

17 See ACCP Conflict Analysis Framework - A Video Illustration. mas-mediation.ethz.ch/tools/accp-conflict-analysis-framework.html

18 Adapted from a draft "ICT considerations in Conflict Analysis" checklist prepared by the United Nations Department of Political and Peacebuilding Affairs. On file with the authors.

- Have there been reports of offensive cyber capabilities deployed to target critical infrastructure or strategic data, deny access to communications or other networks, or implement internet shutdowns?
  - If so, what were the military and non-military effects of the incident or incidents? Have certain communities or parts of society been disproportionately affected (for example, women, refugees, minority populations, specific geographic regions, etc.)?
  - Was or were the incident or incidents publicly attributed to a specific actor? If so, who attributed the incident?
  - Is the claimed perpetrator and/or target of the attack a key party to the conflict?

- Has the government or have the governments in question categorized their critical infrastructure? If so, has it or have they made this categorization public?

- Has the government or have the governments established a national cybersecurity agency and/or a national CERT/CSIRT in the country?

- Has the relevant state (for a civil war) or have the relevant states (for an interstate conflict) expressed support for any international norms relating to the use of offensive cyber capabilities?
  - Does the state or do the states participate in cyber confidence building processes or capacity-building initiatives at the regional level?

The specialized nature of this analysis would likely require peacemakers to take advice from entities such as national or regional CSIRTs/CERTs, CSIRT networks like the Forum of Incident Response and Security Teams (FIRST),[19] academic centers, technology companies, service providers, or specialist consultants. Mediators might also want to invite the conflict parties to information sessions or to conduct shared assessments on the use of offensive cyber capabilities in the conflict as an entry point to discuss and build joint understanding of cyber-related themes. This may be particularly important where there is an asymmetry in cyber capabilities and technical expertise among conflict parties.

19 See first.org/members/teams.

4.1.2. Cyber Process Design Considerations

There is no precedent for how cyber-related issues might be incorporated into negotiation processes to end armed conflict. Broadly speaking, we conceive of two possible alternatives. In the first, restraints on offensive cyber capabilities could be incorporated into the ceasefire talks. Within a broader set of peace negotiations, such ceasefire discussions are often managed in a security-related committee. The alternative would be to conceive of an independent sub-committee specifically for the negotiation of issues relating to offensive cyber capabilities. The latter approach has the advantage of creating a context in which cyber specialists from both sides could meet to discuss the terms of an arrangement, and it also reduces the likelihood that the inclusion of the cyber dimension would serve as a distraction that might delay negotiations to cease conventional conflict. However, this approach also risks relegating the importance of the cyber dimension and increases the likelihood that it might not be properly understood by the political and security leadership of the conflict parties engaged in the broader talks. There would also need to be consideration of how cyber discussions in the security sphere of the mediation process might link to any cyber issues that are raised in negotiations on political or economic issues.[20]

Decisions on this process design question should at least in part be informed by a judgement on how best to manage the challenge posed by the diverse and relatively unfamiliar range of actors that might be need to be involved in cyber ceasefires. In those contexts where cyber operations have been a major feature of the conflict and detailed prohibitions on offensive cyber operations are anticipated, there may be a concomitantly greater rationale to establish a separate sub-committee in talks to facilitate planning for complex implementation arrangements.

On this subject of implementation planning, some conventional ceasefires grant roles to local civil society in civilian ceasefire monitoring. In this respect, practice has shown that the early engagement and integration of civil society actors into the negotiation process is important. The underlying objective of such anticipatory engagement is to generate an informed, consensual, and consultation-based outcome of a ceasefire process by giving civilian partners the opportunity to express their perspectives, concerns, and aspirations in a coordinated manner (United Nations, forthcoming). This

20 As seen in ongoing Libya peace talks, where disinformation and hate speech issues have been explicitly addressed in both the ceasefire and political tracks of the process.

can be critical in ensuring that commitments, prohibitions and ceasefire management modalities will be designed in a more realistic and implementable form while making it more likely that outside actors will fulfil the prospective technical assistance and cyber incident response mandates envisaged for them.

Choices related to the design of the cyber dimension of ceasefire talks also provide an opportunity to expand the inclusivity of such negotiations beyond traditional security sector actors, potentially broadening understanding and the base of support for the agreement among society. There is now substantial evidence that enhanced inclusivity can result in more sustainable and durable peace and ceasefire agreements (Kane, 2019; United Nations, forthcoming). Additionally, the new categories of potential outside actors in cyber ceasefires from the private sector and technical and academic bodies could also offer the chance for more women to make inroads into often male-dominated security talks in peace processes.

4.2. Options for Cyber-related Provisions and Ceasefire Concepts

There are a number of ways in which restraints on offensive cyber operations could be included within a ceasefire. To capture the different options and in recognition that there can be no one-size-fits-all approach, we provide two sets of building blocks.

First, following from our outline in section 3.3 on what is often included in a ceasefire agreement, we provide initial proposals regarding a range of the possible types of commitments, prohibited activities, and ceasefire management and implementation mechanisms that could be prepared with respect to offensive cyber capabilities. To achieve this, we draw inspiration from a number of international efforts to develop cyber norms, rules, principles, and confidence building measures as well as provisions from existing bilateral cyber agreements. Second, using different combinations of these provisions, we utilize Jeremy Brickhill's model of a ceasefire conceptual framework to sketch out several possible Cyber Ceasefire Conceptual Frameworks (CCCFs). These CCCFs aim to capture what Brickhill (2018: 42) calls the "underlying idea" of a ceasefire that should be tailored to the specific nature of a conflict and conflict settlement objectives.

4.2.1. Possible Cyber Ceasefire Provisions and Mechanisms

Since the late 1990s, multiple multilateral and bilateral negotiations as well as non-governmental initiatives have sought to develop norms, principles, and confidence building measures to shape state behavior in cyberspace. To be clear, we do not mean to imply that at present there is international convergence on which cyber actions are permissible and which are prohibited. Nor do we believe that the existing norms, which are often quite general, provide the necessary level of specificity that ceasefire agreements need to respond to the particularities of a given conflict. Rather, we merely suggest that this corpus of norm building represents a useful starting point for negotiators looking for ideas and options to tackle a novel challenge.

A series of six UN Groups of Governmental Experts (GGE), which began in 2004, have led the most prominent of these efforts. In 2015, the fifth GGE produced a consensus report that international law and established legal principles of military necessity, distinction, and proportionality are applicable to cyberspace, along with the UN Charter.[21] It also recommended 11 non-binding political norms of responsible state behavior in cyberspace. These now UN General Assembly endorsed principles (see A/RES/71/28 2016) could serve as reference points for more detailed ceasefire provisions.[22]

Other possible multi-lateral and non-governmental or private sector reference frameworks include the following:

- The Organization for Security and Cooperation in Europe's (OSCE) confidence building measures which focus on information-sharing, voluntary co-operation, and establishment of communication channels to reduce the risks of misperception during cyber incidents;[23]

21 The ICRC further argues that cyber operations during armed conflict are regulated by existing rules of international humanitarian law (ICRC, 2020).

22 The sixth UN GGE composed of 25 states working to to develop further proposed norms on responsible state behavior in relation to the use of digital technologies completed its work just prior to the publication of this study. As of writing, only an unofficial, advance copy of its work has been released. This document expresses particular concern regarding the increasing malicious use of Information and Communication Technologies to influence the "overall stability of another State" and against critical infrastructure. It also further develops the 11 norms from the landmark 2015 GGE Report (see front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf). A separate UN Open Ended Working Group composed of all interested UN member states also issued its final report on these matters in March 2021 (see United Nations, 2021).

23 OSCE Permanent Council Decisions Nos. 1106 (2013) and 1202 (2016).

- The 2009 Shanghai Cooperation Organisation agreement on cooperation in the international information space, which notably contains both cyber-specific definitions and a list of prohibited activities;[24]
- The two Tallinn Manuals, which focus on the international law applicable to cyber warfare and cyber operations, prepared by an independent international group of experts (Schmitt, 2013, 2017). While these Manuals were commissioned by the NATO Cooperative Cyber Defense Centre of Excellence and are hence not universally accepted, they posit detailed principles for potential reference.
- The 2018 Paris Call,[25] which focuses on preventing activity that damages the availability of the public core of the Internet and supports efforts by states, civil society, and the private sector to support victims of the malicious use of Information and Communications Technology (ICT) during and outside of armed conflict.
- The proposal for a new Digital Geneva Convention by Microsoft, which seeks to commit governments not to engage in cyberattacks on the private sector, government services, and civilian infrastructure and to forswear the stockpiling of "zero-day vulnerabilities"[26] (Smith, 2017).

In addition to these multi-lateral efforts, a series of bilateral cyber agreements could provide inspiration for future ceasefires. The most notable are the 2013 Russia-US ICT security cooperation agreement, which takes a transparency and confidence building approach; the 2015 China-US cyber agreement, which entails commitments to timely responses to requests for information and assistance in response to malicious cyber activities; and the 2015 agreement on cooperation between China and Russia, which under some interpretations includes a cyber non-aggression pact and mutual assistance provisions (Korzak, 2015).

With this background, we present some initial proposals to peacemakers for ceasefire provisions related to offensive cyber capabilities. In drawing upon international efforts to develop cyber norms, we follow the UN ceasefire guidance, which suggests consideration of relevant global con-

24 Available at cis-legislation.com/document.fwx?rgn=28340.

25 The Paris Call is composed of 74 states, 333 international and civil society organizations, and 608 private sector entities but does not include China, Iran, Israel, North Korea, Russia or the US.

26 A zero-day vulnerability is a computer-software vulnerability that is unknown to the party or parties responsible for patching or otherwise fixing the flaw until it is actually being exploited as part of an attack (the zero day).

ventions and policy frameworks, as well as international law and international humanitarian law for inclusion in ceasefires (United Nations, forthcoming).

Basic Principles of Constraint on Cyber Operations: These could be included in the sections of the ceasefire agreement focused on declarations of principles. Possible options could include one or some combination of the following:

- a simple statement that the conflict parties commit to observing international law and/or international humanitarian law in respect of their cyber operations;
- an endorsement of the 2015 UN GGE norms (or specific key norms, confidence building measures, and crisis management protocols within them);
- an endorsement of frameworks related to cyberspace developed by regional organizations that the conflict parties are members of (for example the OSCE or the Shanghai Cooperation Organisation); or
- an endorsement of more detailed, non-governmental developed principles such as those in the Tallinn Manuals or the Paris Call.

Cyber-related Communication and Information Sharing Mechanisms: A number of multilateral cyber frameworks and bilateral agreements provide starting points that could be adapted for a ceasefire agreement's section on coordination and management arrangements. Examples include

- voluntary communication, information-sharing, and transparency mechanisms contained in the 2015 UN GGE norms and the OSCE's 16 ICT confidence building measures, including possibly disclosing information regarding the conflict actors' cyber rules of engagement (which are often opaque);
- provisions to share threat indicators between national CERTS/CSIRTS regarding malicious cyber activity that appears to originate from each other's territory and standing mechanisms for communication at technical and senior political levels to reduce the possibility of misperception and escalation (possibly modeled on those contained on the series of bilateral agreements between China, Russia, and the US).

Specific Cyber-related Definitions: There are no universal definitions for conflict-related terminology, and individual ceasefire agreements use similar terms in ways most appropriate for the conflict context and political sensitivities of the actors. This makes clarity in terminology of the utmost importance, so

much so that the inclusion of a glossary or definition of terms is one sign of a technically sound agreement (Haysom & Hottinger, 2004: 4; United Nations, forthcoming). Such a practice has, for example, been attempted in the 2009 Shanghai Cooperation Organisation agreement and the 2015 bilateral China-Russia deal on the "international information space,"[27] which contain annexes defining key ICT terms utilized in the respective texts such as "war," "weapons, "security threat[s]," and "critically important [infra]structures."

Prohibited Acts: All ceasefire agreements include prohibited behaviors, but there is variation in the level of detail provided, including on the scale and the scope of prohibited actions. For a cyber ceasefire agreement, the parties will need to determine what constitutes a cyberattack, which level of severity of attacks is prohibitive, and how this relates to espionage. While there can be no single template for a section dealing with prohibited acts, several options are possible:

- First, parties could prohibit cyberattacks in relation to their effects rather than the technical nature of a cyber operation (Schmitt, 2017: 415). In this sense, cyber operations that can be reasonably expected to cause injury or death to persons or damage or destroy objects could be proscribed (e.g., certain effects of infrastructure or data attacks).
- Second, prohibitions could focus on the target, e.g., proscribing cyberattacks on civilians, civilian objects, and certain types of infrastructure or organizations, such as national CERTs/CSIRTs (Schmitt, 2013; Nye, 2017; United Nations, 2015)
- Thirdly, prohibitions could focus on the operation of particular public and government services. The Paris Call (2018) and the Global Commission on the Stability of Cyberspace (2019), for example, suggest the prohibition of activities that damage the public core or availability of the Internet, which could apply both to a state's efforts to use DDoS attacks to disconnect an adversary from the global Internet (such as with Estonia in 2007) or the use of internet shutdowns in civil conflicts. In a similar vein, Microsoft has proposed norms against cyber operations that result in the disruption of a government's core civilian functions and services (Microsoft, 2019).
- Fourthly, prohibitions could be extended to cyberespionage activities that are hard to distinguish from the implanting of malicious code to conduct future offensive cyber operations. Effectively banning new implants would

27 "International information space" is the preferred nomenclature of Shanghai Cooperation Organisation members for cyberspace.

also make it more difficult to re-start a campaign of cyberattacks quickly and reduce the risk of misunderstanding leading to escalation (Harold, Libicki & Cevallos, 2016: 73). Such a prospective prohibition was reportedly discussed in the 2015 China-US cyber talks (Sanger, 2015), has been a focus in China-US Track II cyber discussions (Harold, Libicki & Cevallos, 2016), and has been publicly called for by senior Russian officials (Markoff & Kramer, 2009). However, it would be exceptionally difficult to monitor or enforce.

- Finally, prohibitions could focus on particular actors, such as proxy forces. This would build on existing practice in ceasefire management, which sometimes requires actors to take responsibility for their proxy forces (Haysom & Hottinger, 2004). The 2015 UN GGE report proposes a norm that states should not use proxies to commit internationally wrongful acts using malicious ICTs or to knowingly allow their territory to be used to do so. The cyber-related literature explores more specific prohibitions. These include commitments by states to close down cyber chat rooms involved in organizing and conducting denial of service attacks, to shut down bot networks hosted on its territory, to commit to end official rhetoric that could be seen as encouraging hacker groups to conduct cyber operations, and to end any funding of and the transfer of software tools to non-state hacker or criminal groups (Healey, 2012a,b). These steps might also be an important move in attempting to manage the potential for spoiler behavior by hardline factions among the conflict parties who may favor the continuation of hostilities.

  Maurer (2018) cautions, however, about the need to be realistic regarding what control state actors can achieve over their proxies. His analysis suggests that signatories to a ceasefire agreement should only expect each other to "manage rather than prohibit" their proxies' activities. Notwithstanding this, he provides examples of China (in 2001) and the US (in 2003) using a combination of public disavowing of hacking campaigns, official statements regarding the illegality of certain hacking activities, and even op-eds from former hackers to reign in cyber proxies (Maurer, 2018: 147, 152).

Commitments to Provide Mutual Assistance: As we have emphasized, monitoring and verifying cyber incidents is notoriously difficult. But within ceasefires, the purpose of incident monitoring and verification is not attribution, accountability, or sanctioning violators per se. Instead, it is to enhance the

credibility and sustainability of the ceasefire by increasing the predictability of the parties' behavior, promoting joint problem solving, and preventing the recurrence of incidents (United Nations, forthcoming). In the cyber realm, we suggest that these functions could, at least in part, be furthered by an emphasis on mutual assistance provisions.

Under this approach, parties could agree to "mutual assistance" provisions in a ceasefire agreement so as to credibly signal a stronger intention to abide by its terms and jointly address problems that arise during implementation. This would create additional self-imposed reputational costs if a party were to renege (as well as some implicit assumption of blame for the incident). Conversely, a conflict party that provides the agreed assistance in the case of a cyber incident would increase trust and reduce the likelihood of the escalation of low-level violations or repetition of genuine accidents. Such provisions could build upon the norm to provide information and assistance in response to malicious cyber activities contained in the 2015 GGE report (especially in the case of attacks on critical infrastructure) and the text of the mutual assistance provision contained in the 2015 China-Russia bilateral agreement.

Ceasefires could also include more specific required actions, such as by signatories committing to cut off malicious internet traffic originating from their own territory in the case of a cyber incident, disabling botnets engaged in DDoS attacks from their territory, or agreeing to co-finance a mixed body of ceasefire signatories and private and non-governmental technical specialists to investigate major cyber incidents. Such investigations would not necessarily be mandated to attribute responsibility for incidents, but they could still act as a disincentive against offensive operations because they could result in the public disclosure of the code and specifics of the cyber tools used in the attack. These are capabilities that actors generally prefer to keep secret so as to preserve their value for future use (Rauscher & Korotkov, 2011; Kavanagh & Cornish, 2020). Finally, the signatories could also agree to co-sponsor requests to third-party or neutral countries to cut off malicious traffic transiting through their jurisdictions.

Setting out the Role for Third Parties: Ceasefire agreements often delegate support and implementation roles to third parties or anticipate ancillary agreements to set out these functions (Haysom & Hottinger, 2004). These roles can include chairing ceasefire management organizations, participating in monitoring mechanisms, and providing technical advice (Brickhill, 2018;

United Nations, forthcoming). Beyond these standard functions, there are multiple ways in which third parties might be involved with the cyber components of ceasefires:

- Cyber operations take place on the networks and systems of private companies. Ceasefire agreements could therefore engage third-party, private network operators to practice what Healey (2012a: 31) refers to as "commercial neutrality" and establish anticipatory mechanisms to coordinate efforts to suppress attack traffic during ceasefire implementation.
- Technical bodies, academic centers, research institutes, and civil society organizations may well be critical to future cyber-related fact-finding or monitoring mechanisms (Kavanagh & Cornish, 2020: 9). Future ceasefire negotiations could thus devote attention to the composition of any envisaged investigative and monitoring teams and to associated protocols for their access to the parties' network systems so that these mechanisms will have maximum credibility. Such teams will likely need to have a mix of different technical profiles and geographic and national backgrounds to enhance their political acceptability to the parties, making CSIRT networks such as Forum of Incident Response and Security Teams (FIRST), which is composed of 575 CERTs/CSIRTs from 97 countries (as of May 2021), a potentially useful resource.
- Increased engagement with state actors that are not party to the conflict may be required. Building on the proposed norm from the 2015 UN GGE report that states should respond to an appropriate request for assistance from another state whose critical infrastructure has been subject to a malicious ICT act, a ceasefire agreement could include a general appeal to certain or all states not to transmit malicious traffic. This appeal could be further endorsed by relevant regional organizations or even the United Nations Security Council. There is precedent for such action, as in certain high-profile civil wars the Security Council has instructed all UN member states to support the implementation of certain aspects of ceasefire or peace agreements.[28]

28 See Security Council resolution 2268 (2016), which endorsed a CoH in Syria. This resolution "urges" all UN member states "to use their influence with the parties to the cessation of hostilities to ensure fulfilment of those commitments and to support efforts to create conditions for a durable and lasting ceasefire."

4.2.2. Possible Cyber Ceasefire Conceptual Frameworks (CCCFs)

Having provided initial options for the individual cyber elements of ceasefire agreements, we turn our attention to how these individual components could be assembled to respond to the particular dynamics and needs of different conflict contexts. As previously noted, in doing so we rely upon Brickhill's (2018) notion of a ceasefire conceptual framework. A ceasefire concept is a summation of the overarching vision of the agreement and what it seeks to accomplish, which should in turn provide guidance for which specific elements should be contained in the agreement and the relationship between the various mechanisms and tools that comprise it. Using this approach, we present four possible CCCFs. These are not mutually exclusive, and elements of them can conceivably be combined. But as specified, these CCCFs embody different conceptual approaches that could be followed to include the cyber domain in a conflict termination process.

4.2.2.1 CCCF 1: "Acknowledgment"

The initial challenge facing peacemakers attempting to incorporate a cyber dimension into ceasefire negotiations is that parties may deny knowledge of, and participation in, these activities. As noted, some of the actors carrying out offensive cyber operations for a conflict party, such as an intelligence agency, may be especially reluctant to participate in formal negotiations. In this context, developing extensive cyber-related ceasefire provisions would be challenging. The first approach to incorporating cyber provisions within a ceasefire could then be obtaining a collective acknowledgment that cyber operations are occurring in the conflict and to ensure that the stopping of cyber activities, even if loosely defined, is understood to be part of a broader cessation of hostilities.

This CCCF could conceivably arise in both inter-state and intra-state contexts and, similar to provisions included within conventional and relatively informal CoH arrangements, would not require detailed specifications of key terms, concepts, and prohibited activities. Nor would this CCCF require the establishment of ceasefire management structures or incident response mechanisms. An Acknowledgement CCCF would not necessarily even require any direct negotiating contact between the conflict parties. Simply *acknowledging the cyber dimension,* and providing a *commitment to cease offensive cyber activities,* does not then require that the parties delve into the profound difficulties associated with proscribing and monitoring activities in cyberspace, nor that the parties accept responsibility for any previous acts. It simply involves a commitment not to undertake any such acts in the future.

A simple commitment to cease cyber operations might be capable of resulting in a reduction in offensive cyber operations and/or reigning in proxy forces, thereby signaling a willingness by parties to explore political negotiations and a more formalized ceasefire to end a conflict. Even without monitoring and verification, the parties may be able to evaluate each other's adherence to these basic commitments if cyber operations are easily detectable by an opponent. For example, if there is an observable reduction in the volume and frequency of cyberattacks and the online distribution of damaging disinformation as compared to prior to the cessation agreement or an end to a distributed denial of service attack or internet shutdown.

4.2.2.2 CCCF 2: "Constraint and Coordination"

An alternative CCCF could be based around constraint and coordination. This is appropriate when conflict parties acknowledge that cyber operations are a feature in the conflict and want to commit to constraining future cyber operations, but lack the capacity, time, or incentives to draft a detailed cyber ceasefire agreement. This conceptual framework calls for the parties to endorse general principles related to cyber operations, establish information-sharing and communication channels to reduce the risks of escalation, and structure future institutional coordination around cyber activities during the ceasefire.

As compared to an Acknowledgement CCCF, this type of agreement would require more specific cyber provisions to be incorporated into ceasefire texts. *Basic principles* of constraint on cyber operations could be set out in sections of an agreement focused on the declarations of principles. Possible textual options for accomplishing this could include one or some combination of the following: a reference to a need to stop all forms of violent activities, including those relating to offensive cyber operations; simple statements by the conflict parties that they will observe international law in respect of their cyber operations; or a more specific endorsement of the 2015 UN GGE or other regional or non-governmental norms.

Turning to *provisions to foster cyber coordination* between parties, the aim here would be to foster new forms of institutional coordination that can manage future cyber incidents that might undermine the ceasefire. As described in section 4.2.1, a number of multilateral cyber frameworks and existing bilateral agreements provide communication and transparency confidence building measures that could be adapted and incorporated into a ceasefire agreement's section on coordination and management arrangements.

4.2.2.3 CCCF 3: "Comprehensive Management"

A third possible CCCF focuses on the comprehensive management of offensive cyber capabilities during conflict. This would be appropriate when cyber capabilities are both a significant feature of a conflict and the parties have a clear desire to scale back these activities. In addition to *basic principles of constraint* and *cyber coordination* mechanisms, a Comprehensive CCCF would call for several more detailed provisions within a ceasefire agreement. As a result, it is likely that a list of *specific cyber-related definitions* would be required for such agreements.

Prohibited acts would be another necessary component of this CCCF. Logically comprehensive CCCFs would demand the greatest specificity on the scale and the scope of prohibited actions. While attempts to agree on prohibited cyber activities is likely to prove contentious, the preceding section provided a series of options for pursuing this task (prohibitions on operations with certain violent or destructive effects, prohibitions on targeting civilians and civilian infrastructure, prohibitions on disrupting internet and public services, prohibitions on new cyber implants in opponents' networks, or prohibitions on proxy activities).

Commitments to mutual assistance could also be important for a comprehensive CCCF. As we have shown throughout this paper, while monitoring, verifying, and attributing responsibility are important to traditional ceasefires, it is very difficult to carry out these functions in cyberspace. If this particular tool of verification and accountability is therefore not feasible for offensive cyber operations, other approaches should be relied upon in its place. Indeed, one practitioner axiom is that ceasefires should not attempt to "monitor the unmonitorable" as this will ultimately detract from the credibility of the ceasefire.[29]

Our main innovation in this respect is for the ceasefire agreement to establish clear mutual assistance obligations in the case of cyber incidents. We have provided several options for mutual assistance provisions, including cutting off malicious traffic originated from territory controlled by one of the parties, co-sponsoring requests to neutral states to take similar steps, and advance funding of mixed investigative teams to study the technical detail of major cyber incidents. We hope that these and other ideas could potentially increase trust, boost the reputational and tactical costs of defecting from cy-

29 Authors' correspondence with Julian Hottinger, January 2021.

ber ceasefire agreements, foster joint problem solving, and thus reduce the likelihood of escalation from misperceptions or low-level incidents.

Setting out the role for third parties is the final area we suggest might be necessary in a comprehensive CCCF. As these agreements are more ambitious, they will likely require support from private sector network operators and software producers during implementation to help mitigate the effect of future incidents; an analogous role for outside states with respect to malicious cyber traffic and proxy activities; and the anticipatory engagement of technical bodies, academic groupings, research institutes, and civil society organizations to assist in incident investigations.

4.2.2.4 CCCF 4: "Cooperation"

Our final possible conceptual cyber ceasefire framework applies to contexts in which a conflict is approaching a comprehensive peace agreement. In this context, conflict parties normally negotiate a definitive ceasefire, a formal agreement at the conclusion of the peace process that sets out how the parties will end the war. In civil war, for example, these agreements can provide for actions such as the disarming and demobilizing of non-state armed groups and a major restructuring of extant security forces to institutionalize cooperation between the former belligerents. Definitive ceasefires are then a key outcome of peace talks, entering into effect alongside a peace agreement covering the political issues underlying a conflict.

A Cooperative CCCF would likely be part of a definitive ceasefire. There likely cannot be a cyber equivalent to conventional disarmament. However, in principle, parties could take pro-active *measures to move from a conflictual to a cooperative relationship.* This might include committing to remove malicious software already implanted in a former adversary's networks by some means or other– or, even more definitively, engaging with former adversaries in a coordinated disclosure of the particular hardware- and software-based network vulnerabilities that were used to gain access to their networks for offensive cyber operations. This would be broadly equivalent to measures in conventional definitive ceasefires that commit the parties to remove any sources of danger to the local civilian population that they were responsible for creating (e.g., minefields).

Would conflict parties ever be willing to disclose this sensitive and valuable information? The negotiation of a definitive ceasefire always requires the incremental disclosure of sensitive information regarding the parties' order of battle (Brickhill, 2018). This involves sharing strategic military

secrets that would make a party vulnerable in the event that their opponent reneged. It is then conceivable that vulnerabilities that were previously used to gain access to an opponent's network could likewise be shared as the parties move towards a more collaborative phase of relations. When considering the feasibility of such disclosures, it should be noted that in some circumstances states already voluntarily choose to disclose vulnerabilities that could be exploited to gain unauthorized access to private companies or other states' networks and systems (Lyngaas, 2015). There has also been international effort to build norms against the stockpiling of such vulnerabilities for military purposes (United Nations, 2015; Paris Call, 2018; Global Commission on Stability in Cyberspace, 2019; Microsoft, 2019). We do not, however, wish to understate the complexity that such disclosures would entail. For example, such steps would likely require the involvement of private sector vendors to patch vulnerabilities relevant to their products. This could raise additional complications, such as reputational damage to the conflict parties and concerns about revealing intelligence sources and methods to private companies.

5. Conclusions

Offensive cyber capabilities are now a part of the conflict landscape. Yet to date, their impact has been relatively limited in comparison to kinetic military approaches. As we noted in the introduction, this leaves scholars of cyber conflict with a dilemma: "overstate the potential lethal and physical harm caused by offensive cyber capabilities in order to secure policy-makers' attention" or characterize cyber capabilities as mostly non-violent and comparatively insignificant and risk overlooking the effect that they can have on a peace process (Shires & Egloff, 2020). In the case of ceasefires specifically, we counsel against this binary framing. Rather than focus on the as yet undemonstrated ability of these technologies to cause death or physical destruction on a large scale, we instead call attention to their potential to undermine a wider ceasefire process if left unregulated. The temptation created by the difficulties in attributing responsibility for cyber operations, the attractiveness of these capabilities as a tool to inflict costs on adversaries, and differing standards between states as to when a cyberattack rises to the threshold of the use of force present new and important risks to the stability of ceasefire regimes.

In response, we have made a first attempt to provide a practical framework for peacemakers working on this novel aspect of contemporary conflict. Our recommendations address what we have identified as a growing need to be prepared to discuss offensive cyber capabilities in ceasefire negotiations. Prior to future ceasefire talks, we recommend that conflict analysis be undertaken to assess the presence or absence of offensive cyber capabilities and operations in the conflict landscape. Where offensive cyber capabilities pose a salient threat to the peace, we believe that they should be incorporated into the process design and substance of ceasefire negotiations and agreements. We have therefore provided some initial considerations and options for accomplishing this task. In this respect, we are in line with the UN Guidance for Effective Mediation. This guide lists "preparedness," which includes the completion of a comprehensive conflict analysis and ensuring that the mediation team possesses the appropriate process design and technical expertise for the specific conflict situation, as a mediation fundamental (United Nations, 2012).

Finally, if conflict parties opt to incorporate restraints on cyber capabilities into a ceasefire agreement, we recommend the development of a conceptual framework to determine the broad goal of the cyber dimension of

the ceasefire. We also elaborate four possible options for cyber ceasefire conceptual frameworks ("Acknowledgement," "Constraint and Coordination," "Comprehensive Management," and "Cooperation") as well as combinations of associated technical provisions.

There will likely be many challenges associated with incorporating cyber capabilities into ceasefire agreements. Given the clandestine nature of most cyber capabilities, there will always be a temptation for conflict parties to keep them confidential as they agree conventional ceasefire provisions, retaining a strategically valuable tool that is hidden from their opponent. And as we discuss in detail, problems loom large with regards to monitoring and verifying cyber incidents, balancing precision with implementability, integrating new classes of participants into ceasefire talks, the non-physical nature of cyberspace, and how to handle cyberespionage.

We therefore offer our proposals as a starting point to invite critical discussion and stimulate further thinking. In debating whether these ideas fall within the realm of the possible, we invite readers to recall the particular context of ceasefire negotiations which aim to end an armed conflict as compared to the more general difficulties entailed in achieving international consensus on regulating offensive cyber capabilities. Successful ceasefire negotiations rely upon political and military judgments by conflicting parties that certain defined commitments and prohibitions are in their common strategic interest at a specified place and time.[30] The success of any such initiative is ultimately rooted in the willingness of the parties to follow up on their commitments rather than discrete enabling tools such as monitoring and verification (United Nations, forthcoming). We submit that when conflict parties have made the strategic decision to explore a negotiated halt to fighting, it should be possible to agree and implement restraints on offensive cyber operations if they are perceived as linked to this broader goal. The responsibility of peacemakers in such circumstances is to assist the conflict parties to prepare for and structure this novel, and increasingly relevant, area of peace negotiations.

30 One comparator may be bilateral arms control treaties, which rely on analogous strategic judgements by their signatories to enter into commitments that go beyond legal or normative obligations (Arimatsu, 2012).

Bibliography

Ackerman, Spencer, Ewen MacAskill & Alice Ross (2015) Junaid Hussain: British hacker for ISIS believed killed in US air strike. *The Guardian* (theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike).

Al Jazeera (2013) Libya protestors force Internet shutdown. *Al Jazeera* (aljazeera.com/news/2013/12/22/libya-protesters-force-internet-shutdown).

Anceschi, Luca (2015) The persistence of media control under consolidated authoritarianism: containing Kazakhstan's digital media. *Demokratizatsiya* 23(3): 277–295.

Arimatsu, Louise (2012) A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. 2012 4th International Conference on Cyber Conflict (ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf).

Barnes, Julian E & Thomas Gibbons-Neff (2019) U.S. carried out cyberattacks on Iran. *The New York Times* (nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html).

BBC News (2013) China IP address link to South Korea cyber-attack. (bbc.com/news/world-asia-21873017).

Beech, Hannah & Saw Nang (2019) The government cut their Internet: Will abuses now remain hidden? *The New York Times* (nytimes.com/2019/07/02/world/asia/internet-shut-down-myanmar-rakhine.html).

Bellovin, Steven M, Susan Landau & Herbert S Lin (2017) Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity* 3(1): 59–68.

Bodeau, Deborah J & Richard D Graubart (2013) Characterizing Effects on the Cyber Adversary. MITRE Technical Report, The MITRE Corporation (mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf).

Borghard, Erica D & Shawn W Lonergan (2019) Cyber operations as imperfect tools of escalation. *Strategic Studies Quarterly* 13(3): 122–145.

Brantly, Aaron F (2018) The cyber deterrence problem. In: Tomáš Minárik, Raik Jakschis & Lauri Lindström (eds) 2018 *10th International Conference on Cyber Conflict: Cycon X: Maximising Effects.* Tallin, NATO CCD COE Publications, 31–54.

Brickhill, Jeremy (2007) Protecting Civilians through Peace Agreements: Challenges and Lessons of the Darfur Peace Agreement. ISS Paper 138, Institute for Security Studies (issafrica.s3.amazonaws.com/site/uploads/Paper138.pdf).

Brickhill, Jeremy (2018) Mediating Security Arrangements in Peace Processes: Critical Perspectives from the Field. CSS Mediation Resources, Center for Security Studies (CSS) at ETH Zurich.

Bronk, Chris & Gregory S Anderson (2017) Encounter battle: Engaging ISIL in cyberspace. *The Cyber Defense Review* 2(1): 93–108.

Buchanan, Ben (2017) *The Cybersecurity Dilemma.* Oxford: Hurst Publishers.

Buchanan, Cate, Govinda Clayton & Alexander Ramsbotham (2021) Ceasefire monitoring: Developments and complexities. Accord Spotlight, Conciliation Resources.

Bund, Jakob (2021) Private correspondence.

Chesney, Robert (2019) Crossing a cyber Rubicon? Overreactions to the IDF's strike on the Hamas cyber facility. *Lawfare* (lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility).

Chounet-Cambas, Luc (2011) Negotiating Ceasefires: Dilemmas & Options for Mediators. Mediation Practice Series, The Centre for Humanitarian Dialogue (hdcentre.org/uploads/tx_news/36Negotiatingceasefires-MPS.pdf).

Clarke, Richard A & Robert Knake (2010) *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins e-books.

Clayton, Govinda, Simon JA Mason, Valerie Sticher & Claudia Wiehler (2019) Ceasefires in intra-state peace processes. *CSS Analyses in Security Policy* (252) (css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse252-EN.pdf).

Clayton, Govinda, Laurie Nathan & Claudia Wiehler (2021) Ceasefire success: A conceptual framework. *International Peacekeeping.* Online first. DOI: 10.1080/13533312.2021.1894934.

Clayton, Govinda & Valerie Sticher (2021) The logic of ceasefires in civil war. *International Studies Quarterly.* Online first. DOI: 10.1093/isq/sqab026

Coombs, Casey (2020) In Yemen, the internet is a key front in the conflict. *Coda Story* (codastory.com/authoritarian-tech/yemen-internet-conflict).

Crocker, Chester A, Fen Osler Hampson & Pamela Aall (2004) *Taming Intractable Conflicts: Mediation in the Hardest Cases.* Washington, DC: United States Institute of Peace Press.

Deibert, Ronald (2015) Authoritarianism goes global: Cyberspace under siege. *Journal of Democracy* 26(3): 64–78.

Deibert, Ronald J, Rafal Rohozinski & Masashi Crete-Nishihata (2012) Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue* 43(1): 3–24.

Egloff, Florian & James Shires (2020) The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence. Working paper presented at the Digital Democracy Workshop, Digital Democracy Lab and Digital Society Initiative, Zurich.

Farrell, Joseph & Matthew Rabin (1996) Cheap talk. *Journal of Economic Perspectives* 10(3): 103–118.

Fortna, Virginia Page (2003) Scraps of paper? Agreements and the durability of peace. *International Organization* 57(2): 337–372.

Fortna, Virginia Page (2004) *Peace Time: Cease-Fire Agreements and the Durability of Peace.* Princeton, NJ: Princeton University Press.

Fulghum, David & Douglas Barrie (2007) Israel used electronic attack in air strike against Syrian mystery target. *ABC News* (abcnews.go.com/Technology/story?id=3702807&page=1).

Gartner, Scott Sigmund & Molly M Melin (2009) Assessing outcomes: Conflict management and the durability of peace. In: Jacob Bercovitch, Victor Kremenyuk & Ira William Zartman (eds) *The SAGE Handbook of Conflict Resolution.* London: SAGE Publications Ltd, 564–579.

Gartzke, Erik (2013) The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security* 38(2): 41–73.

Geers, Kenneth (2011) *Strategic Cyber Security.* Tallin: NATO CCD COE Publications.

Global Commission on the Stability of Cyberspace (2019) *Advancing Cyberstability: Final Report* (cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf).

Gohdes, Anita R (2015) Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research* 52(3): 352–367.

Greenberg, Andy (2017) How an entire nation became Russia's test lab for cyberwar. *Wired* (wired.com/story/russian-hackers-attack-ukraine).

Gunitsky, Seva (2015) Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics* 13(1): 42–54.

Hare, Forrest (2009) Borders in cyberspace: Can sovereignty adapt to the challenges of cyber security? In: Christian Czosseck & Kenneth Geers (eds) *The Virtual Battlefield: Perspectives on Cyber Warfare* Amsterdam: IOS Press, 88–105.

Hare, Forrest (2012) The significance of attribution to cyberspace coercion: A political perspective. In: Christian Czosseck, Rain Ottis & Katharina Ziolkowski (eds) *2012 4th International Conference on Cyber Conflict.* Tallin, NATO CCD COE Publications, 125–139.

Harknett, Richard J & Max Smeets (2020) Cyber campaigns and strategic outcomes. *Journal of Strategic Studies.* Online first. DOI: 10.1080/01402390.2020.1732354

Harold, Scott Warren, Martin C Libicki & Astrid Stuth Cevallos (2016) Getting to Yes with China in Cyberspace. Research Reports, RAND Corporation (rand.org/t/rr1335).

Hart, Kim (2008) Longtime battle lines are recast in Russia and Georgia's cyberwar. *The Washington Post* (washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html).

Hartmann, Kim & Keir Giles (2018) Net neutrality in the context of cyber warfare. In: Tomáš Minárik, Raik Jakschis & Lauri Lindström (eds) *2018 10th International Conference on Cyber Conflict: CyCon X: Maximising Effects.* Tallin, NATO CCD COE Publications, 139–158.

Haysom, Nicholas & Julian Hottinger (2004) Do's and Don'ts of Sustainable Ceasefire Arrangements. Presentation initially presented at the IGAD Sudan peace process workshop on detailed security arrangements in Sudan during the transition and revised for use by peace appeals in Nepal and Sri Lanka. (peacemaker.un.org/sites/peacemaker.un.org/files/DosAndDontofCeasefireAgreements_HaysomHottinger2010.pdf).

Healey, Jason (2012a) When "not my problem" isn't enough: Political neutrality and national responsibility in cyber conflict. In: Christian Czosseck, Rain Ottis & Katharina Ziolkowski (eds) *2012 4th International Conference on Cyber Conflict.* Tallin, NATO CCD COE Publications, 21–33.

Healey, Jason (2012b) Beyond Attribution: Seeking National Responsibility for Cyber Attacks. Issue Brief, Atlantic Council (atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF).

Hollis, David (2011) Cyberwar Case Study: Georgia 2008. Small Wars Journal (smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008).

Hottinger, Julian (2021) Private correspondence.

ICRC (2019) International Humanitarian Law and Cyber Operations during Armed Conflicts. ICRC Position Paper (icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf).

ICRC (2020) Norms for responsible State behavior on cyber operations should build on international law. Statement to the UN Open-ended working group (icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law).

INSIKT Group (2018) Underlying Dimensions of Yemen's Civil War: Control of the Internet. Recorded Future (recordedfuture.com/yemen-internet-activity).

Jun, Jenny, Scott LaFoy & Ethan Sohn (2015) North Korea's Cyber Operations: Strategy and Response. Center for Strategic and International Studies (csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf).

Kane, Sean (2019) Peace Agreement Provisions and the Durability of Peace. CSS Mediation Resources, Center for Security Studies (CSS) at ETH Zurich (css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MediationResources-PeaceAgreements.pdf).

Kavanagh, Camino & Paul Cornish (2020) Cyber Operations and Inter-State Competition and Conflict: The Persisting Value of Preventive Diplomacy. Research in Focus, EU Cyber Direct (eucyberdirect.eu/wp-content/uploads/2020/09/rif-preventive-diplomacy.pdf).

Keremoğlu, Eda & Nils B Weidmann (2020) How dictators control the Internet: A review essay. *Comparative Political Studies* 53(10–11):1690–1703.

King, Gary, Jennifer Pan & Margaret E Roberts (2013) How censorship in China allows government criticism but silences collective expression. *American Political Science Review* 107(2): 326–343.

Korzak, Elaine (2015) Is this China and Russia's 'nonaggression pact' for cyberspace? *The National Interest*(nationalinterest.org/blog/the-buzz/china-russias-nonaggression-pact%E2%80%9D-cyberspace-13654).

Kostyuk, Nadiya & Yuri M Zhukov (2019) Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution* 63(2): 317–347.

Landler, Mark & John Markoff (2007) In Estonia, what may be the first war in cyberspace. *The New York Times* (nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html).

Lewis, James A (2011) Rethinking Cybersecurity – A Comprehensive Approach. Speech given at the Sasakawa Peace Foundation (csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/110920_Japan_speech_2011.pdf).

Liles, Samuel (2010) Cyber warfare: As a form of low-intensity conflict and insurgency. In: Christian Czosseck & Karlis Podins (eds) *Conference on Cyber Conflict: Proceedings 2010.* Tallin, NATO CCD COE Publications, 47–57.

Lin, Herbert S (2010) Offensive cyber operations and the use of force. *Journal of National Security Law & Policy* 4(1) 63–86.

Lin, Herbert (2012) Cyber conflict and international humanitarian law. *International Review of the Red Cross* 94(886): 515–531.

Lin, Herbert (2016) Attribution of malicious cyber incidents: From soup to nuts. *Journal of International Affairs* 70(1): 75–137.

Lindsay, Jon R (2013) Stuxnet and the limits of cyber warfare. *Security Studies* 22(3): 365–404.

Lindsay, Jon R (2017) Restrained by design: The political economy of cybersecurity. *Digital Policy, Regulation and Governance* 19(6): 493–514.

Lyngaas, Sean (2015) NSA chief says agency discloses '91 percent' of zero day bugs. *Federal Computer Week* (fcw.com/articles/2015/11/09/rogers-zero-days-nsa-lyngaas.aspx).

Markoff, John (2008) Before the gunfire, cyberattacks. *The New York Times* (nytimes.com/2008/08/13/technology/13cyber.html).

Markoff, John & Andrew E Kramer (2009) U.S. and Russia differ on a treaty for cyberspace. *The New York Times* (nytimes.com/2009/06/28/world/28cyber.html).

Marks, Joseph (2015) ISIL aims to launch cyberattacks on U.S. *Politico* (politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179).

Maschmeyer, Lennart (2020) Slow Burn: Cyber Conflict and Subversion in Ukraine. Working paper.

Maurer, Tim (2011) The case for cyberwarfare. *Foreign Policy* (foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare).

Maurer, Tim (2018) *Cyber Mercenaries: The State, Hackers, and Power.* Cambridge: Cambridge University Press.

Microsoft (2019) Protecting People in Cyberspace: The Vital Role of the United Nations in 2020 (un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf).

Melman, Yossi (2020) Iran struck first. 'Israel' retaliated massively. Behind the cyber war rattling the Middle East. *Haaretz* (haaretz.com/israel-news/iran-israel-cyber-war-middle-east-mossad-persian-gulf-port-1.8858292).

Morrow, James D (1999) How could trade affect conflict? *Journal of Peace Research* 36(4): 481–489.

Nakashima, Ellen (2011) U.S. cyberweapons had been considered to disrupt Gaddafi's air defenses. *Washington Post* (washingtonpost.com/world/national-security/us-cyber-weapons-had-been-considered-to-disrupt-gaddafis-air-defenses/2011/10/17/gIQAETpssL_story.html).

Newman, Lily Hay (2019) What Israel's strike on Hamas hackers means for cyberwar. *Wired* (wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar).

Nye, Joseph S (2017) Deterrence and dissuasion in cyberspace. *International Security* 41(3): 44–71.

Organisation for Security and Co-operation in Europe. Permanent Council Decision No. 1106. Vienna: OSCE, December 3, 2013. (osce.org/files/f/documents/d/1/109168.pdf).

Organisation for Security and Co-operation in Europe. Permanent Council Decision No. 1202. Vienna: OSCE, March 10, 2016. (osce.org/files/f/documents/d/a/227281.pdf).

Paris Call for Trust and Security in Cyberspace (2018). (pariscall.international/en).

PILPG (2013) The Ceasefire Drafter's Handbook. Public International Law & Policy Group (publicinternationallawandpolicygroup.org/s/PILPG-Ceasefire-Drafters-Handbook-IncludingTemplateCeasefireAgreement-2-7es4.pdf).

Potter, Antonia (2004) Ceasefire Monitoring and Verification: Identifying Best Practice. Background paper presented at Mediator's Retreat, Oslo. Centre for Humanitarian Dialogue (hdcentre.org/wp-content/uploads/2016/07/Ceasefire-Monitoring-and-Verification-Identifying-Best-Practice-June-2004.pdf).

Kyaw Lwin Oo (2019) Rights groups: Internet shutdown in Myanmar's Rakhine hampers aid work, causes hardship. *Radio Free Asia* (rfa.org/english/news/myanmar/rights-groups-internet-shutdown-07222019155332.html).

Ralph, Talia (2013) Syria's Electronic Army attempted attack on Haifa's water system. *GlobalPost* (pri.org/stories/2013-05-25/syrias-electronic-army-attempted-attack-haifas-water-system).

Rauscher, Karl Frederick & Andrey Korotkov (2011) Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace. EastWest Institute (eastwest.ngo/sites/default/files/ideas-files/US-Russia.pdf).

Rid, Thomas & Ben Buchanan (2015) Attributing cyber attacks. *Journal of Strategic Studies* 38(1–2): 4–37.

Rød, Espen Geelmuyden & Nils B Weidmann (2015) Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research* 52(3): 338–351.

Sanger, David E (2015) U.S. and China seek arms deal for cyberspace. *The New York Times* (nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html).

Sanger, David E & Emily Schmall (2021) China appears to warn India: push too hard and the lights could go out. *The New York Times* (nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html)

Sanger, David E, Eric Schmitt & Ronen Bergmann (2020) Long-planned and bigger than thought: Strike on Iran's nuclear program. *The New York Times* (nytimes.com/2020/07/10/world/middleeast/iran-nuclear-trump.html).

Satter, Raphael (2012) US general: We hacked the enemy in Afghanistan. *Associated Press* (news.yahoo.com/us-general-hacked-enemy-afghanistan-161426332.html?guccounter=1).

Schmitt, Eric & Julian E Barnes (2019) White House reviews military plans against Iran, in echoes of Iraq War. *The New York Times* (nytimes.com/2019/05/13/world/middleeast/us-military-plans-iran.html).

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

Schmitt, Michael N, ed (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd Ed.). Cambridge: Cambridge University Press.

Shimeall, Timothy, Phil Williams & Casey Dunlevy (2001) Countering cyber war. *NATO Review* (nato.int/docu/review/articles/2001/12/01/countering-cyber-war/index.html).

Shires, James (2020) The simulation of scandal: Hack-and-leak operations, the Gulf States, and U.S. politics. *Texas National Security Review* 3(4) 10–28 (tnsr.org/2020/08/the-simulation-of-scandal-hack-and-leak-operations-the-gulf-states-and-u-s-politics).

Shires, James & Max Smeets (2017) The word *cyber* now means everything – and nothing at all. *Slate* (slate.com/technology/2017/12/the-word-cyber-has-lost-all-meaning.html).

Smeets, Max (2018) The strategic promise of offensive cyber operations. *Strategic Studies Quarterly* 12(3): 90–113.

Smith, James DD (1995) *Stopping Wars: Defining the Obstacles to Cease-Fire.* Boulder, CO: Westview Press.

Smith, Brad (2017) The need for a Digital Geneva Convention. *Microsoft On the Issues* (blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention).

Stein, Georg (2019) In Dire Straits: The State of Literature on Ceasefire Negotiations and Mediation. *Unpublished paper submitted to ETH Zurich.* On file with authors.

Taye, Berhan (2019) The State of Internet Shutdowns around the World: The 2018 #KeepItOn Report. (accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf).

Taye, Berhan (2020) Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019. (accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf).

Thomas, Elise & Albert Zhang (2020) Snapshot of a shadow war in the Azerbaijan–Armenia conflict. *The Strategist – The Australian Strategic Policy Institute Blog* (aspistrategist.org.au/snapshot-of-a-shadow-war-in-the-azerbaijan-armenia-conflict).

Tikk, Eneken, Kaska Kadri & Vihul Liis (2010) *International Cyber Incidents: Legal Considerations* (1st Ed.). Tallinn, NATO CCD COE Publications.

Toft, Monica Duffy (2010) Ending civil wars: A case for rebel victory? *International Security* 34(4): 7–36.

Tønnesson, Stein (2021) Facebook's power in Myanmar. *PRIO Blogs* (blogs.prio.org/2021/02/facebooks-power-in-myanmar).

United Nations (2012) *UN Guidance for Effective Mediation | UN Peacemaker.* New York: United Nations Publications (peacemaker.un.org/guidance-effective-mediation).

United Nations (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (digitallibrary.un.org/record/799853?ln=en).

United Nations. S/RES/2268. New York: United Nations, February 26, 2016. (unscr.com/en/resolutions/doc/2268).

United Nations. A/RES/71/28. New York: United Nations, December 5, 2016. (undocs.org/A/RES/71/28).

United Nations (2021) Final Substantive Report of Open-ended working group on developments in the field of information and telecommunications in the context of international security (front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf).

United Nations (forthcoming) United Nations Guidance of Ceasefires, draft.

Verjee, Aly (2019) Monitoring Ceasefires Is Getting Harder: Greater Innovation Is Required. Winning essay of the Oslo Forum Peacewriter Prize in 2019, The Centre for Humanitarian Dialogue (hdcentre.org/wp-content/uploads/2019/07/Oslo-Forum-Peacewriter-Prize-2019.pdf).

von Heinegg, Wolff Heintschel (2012) Legal implications of territorial sovereignty in cyberspace. In: Christian Czosseck, Rain Ottis & Katharina Ziolkowski (eds) *2012 4th International Conference on Cyber Conflict.* Tallin, NATO CCD COE Publications, 7–19.

Weber, Valentin (2018) States and their proxies in cyber operations. *Lawfare* (lawfareblog.com/states-proxies-cyber-operations).

Werner, Suzanne & Amy Yuen (2005) Making and keeping peace. *International Organization* 59(2): 261–292.

Zetter, Kim (2016) Everything we know about Ukraine's power plant hack. *Wired* (wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack).

CSS Mediation Resources is a series that aims to provide methodological guidance and insights to mediators, negotiators, and peace practitioners working to address violent political conflicts. It is produced by the Mediation Support Team of the Center for Security Studies at ETH Zurich, with contributions from occasional guest authors. Previous issues include:

- Peace Agreements and Disarmament, Demobilization and Reintegration (DDR): Insights from the Central African Republic and Libya (2021)
- Peace Agreement Provisions and the Durability of Peace (2019)
- Addressing Religion in Conflict: Insights and Case Studies from Myanmar (2018)
- Mediating Security Arrangements in Peace Processes: Critical Perspectives from the Field (2018)
- Preventing Violence: Community-based Approaches to Early Warning and Early Response (2016)
- Gender in Mediation: An Exercise Handbook for Trainers (2015)
- Approaching Religion in Conflict Transformation: Concepts, Cases and Practical Implications (2015)
- Inside the Box: Using Integrative Simulations to Teach Conflict, Negotiations and Mediation (2015)
- Mediating Water Use Conflicts in Peace Processes (2013)
- Swiss Civilian Peace Promotion, Assessing Policy and Practice (2011)
- Mapping Mediators, A Comparison of Third Parties and Implications for Switzerland (2011)
- Mediating Tensions over Islam in Denmark, Holland, and Switzerland (2010)
- To Be a Negotiator, Strategies and Tactics (2009)
- Unpacking the Mystery of Mediation in African Peace Processes (2008)

Mediation Support Project

The goal of the Mediation Support Project (MSP) is to improve the effectiveness of Swiss and international peace mediation. The MSP was established in 2005 as a joint venture between the Swiss Peace Foundation (swisspeace) and the Center for Security Studies (CSS) at ETH Zurich. The MSP is a service provider to the Swiss Federal Department of Foreign Affairs (FDFA), but also to mediators and conflict parties that are strategically important for the FDFA.

The Center for Security Studies (CSS) at ETH Zurich

The CSS is a center of competence for Swiss and international security policy. It offers security and peace policy expertise in research, teaching, and consultancy.

Published with the support of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

"In this groundbreaking study, Sean Kane and Govinda Clayton recognise that offensive cyber capabilities are part of the landscape of armed conflict today and could grow into a more prominent feature of tomorrow's hybrid conflicts. They call attention to cyber's capacity to undermine and disrupt a wider ceasefire process and offer practical advice for peacemakers to incorporate the cyber dimension into the design and substance of ceasefire negotiations and agreements. Essential reading for the future of conflict mediation."
Teresa Whitfield, Director of the Policy and Mediation Division of the UN Department of Political and Peacebuilding Affairs

"Technological innovation brings about opportunities as well as challenges: Cyberattacks are part of a new reality of conflict that we are forced to take into consideration in our peace building work."
Ambassador Simon Geissbühler, Peace and Human Rights Division, Swiss FDFA

"Nowadays, most conflicts have cyber-components that directly or indirectly influence conflict dynamics. It is of great value to think about what those cyber aspects are and how they can be addressed through peace building efforts."
Myriam Dunn Cavelty, Senior Lecturer for Security Studies and Deputy for Research and Teaching at the Center for Security Studies (CSS)

"A fascinating and groundbreaking study establishing a thoughtful and practical introductory framework to address a new and largely unknown and unfamiliar form of conflict, this study not only explores and uncovers the challenges to ceasefire design and management posed by cyber warfare, it thoroughly demonstrates the application of appropriate analytical and technical preparation to process design in any ceasefire negotiation process."
Jeremy Brickhill, Author of "Mediating Security Arrangements in Peace Processes: Critical Perspectives from the Field"