Positioning diplomacy within a strategic response to the cyber conflict threat

Karen Renaud
Amel Attatfa
Tony Craig

Renaud, K., Attatfa, A. & Craig, T. (2022) 'Positioning diplomacy within a strategic response to the cyber conflict threat'. In: S. Parkin & L. Viganò (eds.) *Socio-Technical Aspects in Security: 11th International Workshop, STAST 2021, virtual event, October 8, 2021*. Springer, Cham, pp. 131-152, 11th International Workshop on Socio-Technical Aspects in Security, 8 October 2021.

Positioning Diplomacy within a Strategic Response to the Cyber Conflict Threat

Karen Renaud[1,2,3,4][0000−0002−7187−6531], Amel Attatfa[2][0000−0001−7875−7933], and Tony Craig[1][0000−0003−4497−9831]

[1] University of Strathclyde, Glasgow, UK.
{karen.renaud;anthony.craig}@strath.ac.uk
[2] Abertay University, Dundee, UK. a.attatfa1900@abertay.ac.uk; amel.attatfa.cybdip@gmail.com
[3] Rhodes University, Grahamstown, RSA
[4] University of South Africa, Gauteng, RSA

Abstract.
Background. Nation states unleash cyber attacks targeting other nation states (e.g. WannaCry, SolarWinds), termed "offensive cyber operations". When such aggressions are deemed, according to the UN Charter, to constitute *a threat to the peace, breach of the peace, or act of aggression towards a nation state*, governments might choose to respond. Responses can range from silence all the way to retaliation, at the other end of the scale. The emergence of cyber diplomacy suggests a less militant and potentially powerful response option. Barrinha and Renard [5] explain that the rise of cyber diplomacy has coincided with "a growing contestation of the values, institutions and power dynamics of the liberal-created cyberspace". (p.3). The question is: how could cyber diplomacy fit into a strategic threat management plan?

Aim. To position cyber diplomacy within a strategic response to nation state offensive cyber operations.

Method. To help us to position cyber diplomacy's role in this domain, we first examine historical cyber conflicts, and governments' responses to these, as well as testing the factors that might explain response choice. We then review a number of proposed options for managing cyber conflicts.

Results. We propose a comprehensive "Five D's" strategic framework to manage the threat of offensive cyber operations. Cyber diplomacy is included, acknowledging its emerging and potentially powerful role in managing cyber conflicts in the future.

Conclusions. Cyber diplomacy has recently emerged and it has not yet been widely deployed. We show how it can be positioned within a strategic framework for managing the threat of offensive cyber operations from other nation states.

Keywords: Offensive Cyber Operations, Cyber Diplomacy, Strategic Management of Threats

1 Introduction

Cyber attacks can be perpetrated by a range of agents, including script kiddies, cyber criminal gangs and nation states [25]. The targets, too, range from individual citizens [50], to companies [47] all the way to nation states. It is increasingly clear that this is a present and serious threat [11, 29], which Barker says has increased 100% over the last 3 years [4]. In this paper, we are interested in nation states targeting other nation states in the cyber realm, to "*disrupt their peace*"[1]. Sigholm and Larsson [61] argue that these kinds of attacks are a natural extension of traditional military and intelligence operations to the cyber arena.

In 1996, USA President Clinton established the Commission of Critical Infrastructure Protection[2]. He wanted to ensure that electricity communications and computer networks would be protected from attack[3]. At the time, no one could have anticipated the likes of the wide-ranging SolarWinds cyber attack of 2020 [68], which did indeed impact electricity utilities [74]. Using Lin's terminology of an "*offensive cyber operation*" [39] to describe 'nation state on nation state' cyber aggressions, we will refer to these events as **OCO**s in this paper.

The cyber conflict database published by Valeriano and Maness [73] lists 266 OCOs that occurred from 2000 to 2016, confirming the reality of the threat. The actual incidence is likely to be even higher, given significant under-reporting [31].

Article 51 of the UN Charter gives countries the right of self-defense, permitting forceful responses to "armed attacks"[4], which includes cyber aggressions [58]. Even so, most of these cyber-related incidents do not trigger any significant response from the target country [41].

Governments have a number of options in responding to OCOs [3, 42]. Our focus, in this paper, is on the deployment of cyber diplomacy, which can be defined as "*the use of diplomatic tools and the diplomatic mindset to resolve issues arising from cyberspace*" [1, p. 60]. We commenced by exploring the nature of governments' responses to OCOs, the factors that trigger these, and the occurrence of diplomatic responses. We then considered various proposed strategies for managing the OCO threat, including diplomacy. Finally, we produced a proposed framework for managing OCO threats, which includes cyber diplomacy. Our research questions are thus:

RQ1: *Which factors influence responses to OCOs, and how often was diplomacy the response?*

RQ2: *What proposals have been advanced for managing OCO threats on a global scale?*

RQ3: *How could cyber diplomacy fit into a strategic response to the OCO threat?*

Section 2 reviews the related literature and identifies factors that are likely to influence responses to OCOs. Sections 3, 4 and 5 address RQ1, RQ2 and RQ3 respectively, cultimating in the "Five D's" strategic framework for managing OCO threats. Section 6 discusses the paper's findings and concludes, with Section 7 acknowledging the limitations of our empirical investigation.

2 Background: Nation State Cyber Aggressions

We commence by defining OCOs, to ensure that this discussion is well grounded. Lin [39] defines an OCOs as: "*military operations and activities in cyberspace for cyber attack against and (or) cyber-exploitation of adversary information systems and networks*". This umbrella term including cyber attacks and exploitations, which can be destructive or non-destructive (e.g. espionage).

What distinguishes OCOs from cyber attacks that target individual computer users or companies? Murray [43] argues that cyber aggressions targeting "citizenry", as opposed to "individual citizens", are characterised by the intention to harm the target *nation* by denying it the use of its resources. OCOs may disrupt essential services (e.g., WannaCry[5] which disrupted the UK's National Health Service), destroy resources (e.g., the Stuxnet[6] OCO on Iran's nuclear centrifuges), manipulate information or information systems (e.g. the SolarWinds[7] supply chain OCO), or steal intelligence [52]. Sometimes, the impact cascades into the physical domain, as occurred in the Not-Petya cyber aggression [22], affecting the lives of significant numbers of Ukrainian citizens.

Pomerlau [52] explains that cyber attacks from non-state actors generally aim to coerce targets or gain financially. Attacks by nation states targeting other nation states, on the other hand, are motivated by geopolitics. Rosenzweig [57] presents a typology of cyber aggressions, in terms of the mass harm caused. He commences with cyber mischief at the lowest level advancing to cyber crime, cyber espionage, cyber terrorism and cyber war harming the most citizens of the target country. As such, the closer one gets to the top of Rosenzweig's typology, the more likely it is that the nation state is the target, and governments might feel compelled to respond in some way.

2.1 Choosing a Response

Baram and Sommer [3] suggest a range of responses to OCOs, based on whether governments: (1) admit the OCO occurred (e.g., [9]), (2) attribute the OCO to a country, (3) both[8] or (4) neither[9]. It is worth emphasising that attribution is challenging [18, 59]. Countries might engage, directly or indirectly, via a third party, or camouflage their OCO. [35,56,70]. If governments *do* decide to attribute an OCO to the aggressive actions of another state, Moret and Pawlak [42] provide a long list of potential responses, which *does* include diplomacy, but also includes a military response at the upper end of the scale.

Response Choice Architecture: We currently have little understanding of the factors that might influence the choice of response. As a first foray, we identify four dimensions of the choice architecture that could be influential. These are: (1) the attributes of the state-sponsored aggressor, (2) the severity of the cyber operation, (3) the relations between the two countries, and (4) the attributes of the target state. There are undoubtedly many others, which could be the focus of future research. Yet, these offer a broad framework for exploring the nature of responses to OCOs.

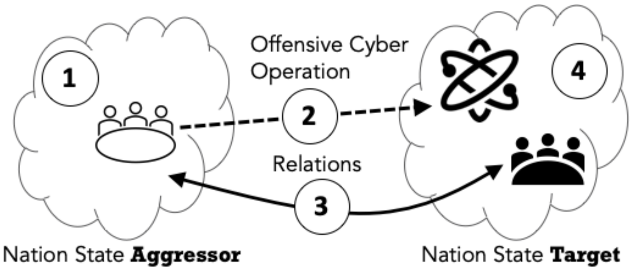

Fig. 1. Four dimensions influencing the choice of response to an OCO: (1) Aggressor, (2) OCO Severity, (3) Aggressor vs. Target, (4) Target

First, the aggressor (#1 in Figure 1). **(1)** The power of the state sponsor of an OCO could shape the response from the target state [2]. Some approaches in the International Relations literature suggest that a country's power allows it to influence the behaviour of others [77]. With no international arbiter of conflict, the balance of power between states is what determines who can do what to others. A powerful state could therefore be better able to deter harsher responses from the recipient of a cyber operation.

Second, the OCO (#2 in Figure 1). **(2)** the severity of the OCO is likely to be influential in terms of triggering a response. Analysts have drawn a distinction between cyber operations that are exploitative and those that are destructive [34, 39]. Exploitative operations, such as acts of cyber espionage, aim to observe or exfiltrate data from the target's computer systems. Destructive attacks aim to change or destroy computer systems, or the information stored within them. Another distinction made by scholars is between "low-cost, low-payoff" disruptions and "high-cost, high-payoff" attacks against critical infrastructure targets [72]. We might expect more severe OCOs to trigger proportionally robust responses from target states as they try to deter further harm via punishment mechanisms [46, p.55].

***Third*, (3)** (#3 in Figure 1) pre-existing diplomatic relations between the aggressor and target nations. Pairs of countries that have closer diplomatic relations may have more communication channels available to resolve incidents peacefully. A lack of diplomatic relations might trigger a more robust response.

Fourth, the target country's characteristics (#4 in Figure 1).

(4a) The general level of Internet dependence in a country could feed into perceived vulnerability, threat, and thus the kind of response to an OCO The more devices connected to the Internet, the more extensive the attack surface and thus greater potential harm from OCOs [37]. For example, North Korea has an advantage over the United States in the event of a cyber war, given the differences in Internet dependence [63, p.151]. With more potential for cyber security breaches, a state may be increasingly motivated to punish OCOs and deter them in the future.

(4b) The power of the target country, approximated by its Gross Domestic Product (GDP). States with more economic power are likely to have the capacity to adopt robust responses. Powerful states also have more motivation to retaliate to protect their prestige.

(4c) Power in international relations is related to the alliance partnerships that states can draw on to project influence or deter OCOs. Without the resources or alliances, weaker states in international politics will be limited in how they can respond to an OCO.

3 RQ1: Historical Responses

In this section, we seek to scope the influence of the aforementioned factors on governments' responses to OCOs. This analysis is inductive rather than theory directed, due to the absence of existing theories to build on. The proposed model is depicted in Figure 2, with variables detailed in Table 1.

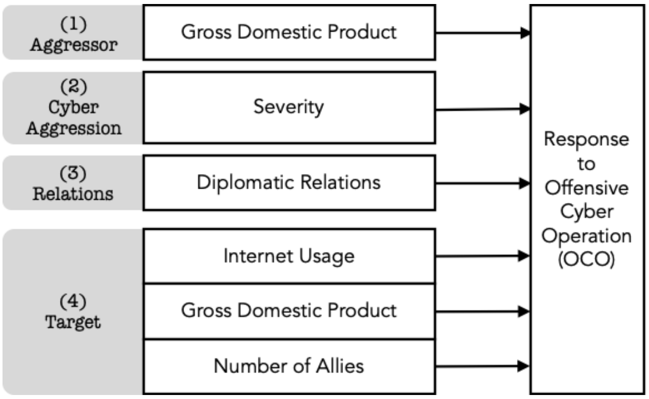

Fig. 2. Proposed model of factors influencing responses to OCOs

3.1 Methods

We draw on data from the Council on Foreign Relation's Cyber Operations Tracker. At the time the data was downloaded in 2020, the Cyber Operations Tracker data included 481 OCOs from 2005 to 2020. These are limited to publicly known, state-sponsored OCOs (OCOs). Of these 482 OCOs, the response chosen by the target state was recorded for 86 instances.

Given the limitations of this data, we do not claim generalisation possibilities. Until more data comes to light, however, the Cyber Operations Tracker provides the only source of information on cyber operations *and* governments' responses to them. We therefore use this data source to discover if there are any correlations

Table 1. Measurement of Variables

Variable	**Measurement**
(1) Aggressor Power: The wealth of the OCO aggressor will influence the robustness of the response to an OCO.	We used the GDP of the aggressor state (constant 2010 USA dollars) as a measure of its wealth and power.
(2) OCO Severity: The more destructive an OCO, the stronger the response from the target government	We relied on the variable provided by the Cyber Operations Tracker, which classifies attack mechanisms as defacement, distributed denial of service (DDoS), doxing, espionage, financial theft, data destruction, sabotage, and multiple (Definitions provided on the Cyber Operations Tracker (CFR) website[10]. To simplify severity analysis, we recoded this information as either *destructive* or *non-destructive*, which maps onto the distinction made by Lin [39]. Destructive OCOs either cause damage to physical infrastructure or to data, and include data destruction and sabotage. Non-destructive attacks include defacement, DDoS, doxing, espionage, and financial theft. There was one instance where the type of OCO was coded as "several", which we re-coded as "missing".
(3) Diplomatic Relations: The weaker the diplomatic relations between the target and aggressor, the more robust the response from the target to an OCO	We used data on diplomatic exchanges from the Correlates of War [6] that indicates if a country has any diplomatic presence in another, including *charges d'affairs*, ministers, or ambassadors, or else has zero diplomatic representation in another country. The data ends in the year 2005 it may reflect an historical rather than present state of relations.
(4a) Target's Internet Use: The more citizens using the internet, the larger the vulnerable attack surface.	As a proxy for Internet dependence, we used World Bank data on the percentage of the country's population that has used the internet in the past 12 months.
(4b) Target Power: The wealth of the OCO target will influence the robustness of the response to an OCO.	We used the GDP of the target state (constant 2010 USA dollars) as a measure of its wealth and power.
(4c) Target's Allies: Target countries with more international allies should adopt more robust responses to OCOs	We counted the number of defence pacts each target country had signed using the formal alliances (v4.1) dataset from the Correlates of War [6]. A defence pact is determined if a signed treaty between states includes providing defence to one or more state involved.

between our selected factors and the nature of the response chosen in response to an OCO.

We analyse this incident-level data set where each row gives information about one of these 86 OCOs as well as the target state and the state aggressor. In some cases, multiple countries are listed as targets. In these cases, there were also responses from multiple targets, so the number of observations in the data set was expanded so there is a unique row of data for each involved government. The data set thus expanded to 91 observations.

3.2 Dependent variable: State response to OCO

Our dependent variable is a binary measure of the type of response a state has taken in responding. For this we recode the information provided by the Cyber Operations Tracker, which categorises target government responses into seven types as described in Table 2. Denouncement is the most common response and is evident in 53.5% of OCOs.

Table 2. Frequency of target government response variable

Type of response	Freq	%
Denial	1	1.1
Confirmation	14	15.4
Denouncement	49	53.9
Criminal charges	17	18.7
Sanctions	6	6.6
Hack-back	2	2.2
Unknown	2	2.2
Total	91	100.0

Table 3. Frequency of re-coded target government response variable

Type of response	Freq	%
Active (criminal charges, sanctions, hack-backs)	25	28.1
Passive (denial, confirmation, denouncement)	64	71.9
Total	89	100.0

To create a simpler indication of the strength of response that is more amenable to logistic regression analysis, we recoded the range of responses into two categories: (1) active, and (2) passive. Responses where the state takes action against the state sponsor of the OCO are coded as ‘active’, and include criminal charges, sanctions, hack-backs and diplomacy. Responses where the state did not take action against the state sponsor are coded as ‘passive’, and include denial, confirmation, and denouncement. The scale of response is therefore a binary variable taking one of two values: 0 or 1, where 1 indicates a stronger response from the target state. There are two instances where there was a suspected response, yet the precise actions were unspecified. These are coded as ‘missing’, leaving the final number of cases assessed at 89. Table 3 shows that more robust, active responses occur 28.1% of the time. In the next section, we describe the results of a logistic regression model where we measure the effect that each factor has on the likelihood of a state adopting a more active response to a cyber attack.

3.3 Empirical Findings

Table 4 provides the results of the logistic regression analysis, examining the effect of each of our factors on the scale of response taken by the target of an OCO. The coefficient shows the change in the odds of the target state carrying out an active response if there is a one unit increase in the value of each independent variable, while controlling for the effects of the other independent variables. An odds ratio above 1 indicates a positive relationship between the independent variable and the robustness of response, while a ratio below 1 indicates a negative association. For each independent variable, the coefficient is displayed along with the robust standard error, the p value indicating statistical significance at the 95% confidence level, and the lower and upper confidence interval limits. P values under 0.05 are considered statistically significant ($p<0.05$). The model uses listwise deletion of missing values which limits the analysis to 64 observations when all variables are included in the same model. The first factor we test is the economic power of the suspected state sponsor of the OCO, measured by its GDP. Despite a slight positive relationship, the result is not statistically significant. The power of the aggressor therefore does not seem to have a deterrent effect on the kind of response chosen by the target. The severity of the OCO is not a good predictor of diplomatic response type either.

Table 4. Logistic regression of cyber response type (active or passive)

Independent variable	Coefficient (Odds Ratio)	Robust standard error	P value	Lower 95% Confidence level	Upper 95% Confidence level
Aggressor's GDP (Log)	1.13	0.36	0.696	0.61	2.10
Severity of OCO	1.12	1.49	0.931	0.08	15.07
Diplomatic relations	0.63	0.70	0.677	0.07	5.67
Internet usage of target (%)	1.05	0.04	0.217	0.97	1.15
Target's GDP (Log)	1.56	0.60	0.251	0.73	3.31
Number of allies of target	1.29	0.16	0.042	1.01	1.65
Constant	0.00	0.00	0.065	0.00	4.20

Note: 64 observations. Constant estimates baseline odds. GDP of aggressor and target is log transformed to reduce skew.

For each independent variable, the coefficient is displayed along with the robust standard error, the p-value indicating statistical significance at the 95% confidence level, and the lower and upper confidence interval limits. P-values under 0.05 are considered statistically significant ($p<0.05$). The model uses listwise deletion of missing values which limits the analysis to 64 observations when all variables are included in the same model.

The first factor we test is the economic power of the suspected state sponsor of the OCO, measured by its GDP. Despite a slight positive relationship, the result is not statistically significant. The power of the aggressor therefore does not seem to have a deterrent effect on the kind of response chosen by the target. The severity of the OCO is not a good predictor of diplomatic response type either.

This suggests that destructive OCOs which damage digital or physical infrastructure do not invoke a more active response than non-destructive OCOs, such as website defacement, DDoS, or espionage. It is possible that states view certain non-destructive OCOs as equally threatening to their national security. Cyber espionage, for instance, can cause serious economic and reputational harm, which might lead to similar responses to those in response to destructive OCOs. Indeed, there is ongoing debate on whether cyber espionage should be seen as part of norm inter-state interactions or whether it warrants a military response [66].

There is a negative correlation between mutual diplomatic representation between the target and state-sponsor of an OCO and the chosen response, shown by a coefficient below 1, but it is very small and statistically insignificant. The nature of cyber responses therefore does not seem to be influenced by pre-existing diplomatic relations, at least under this metric. It is likely that most nation states engaged in cyber conflict already have poor relations or are engaged in strategic rivalry, in which case diplomatic relations may be less relevant.

The fourth factor is the level of internet usage in the target state. Again, there is a very low association between the percentage of the population using the internet and the robustness of the OCO response, which lacks statistical significance. Responses to OCOs do not increase in severity with increases in internet usage.

The target state's power, approximated by its GDP (constant US dollars) is our next factor. Here we see a larger coefficient, suggesting a positive association between the victim's GDP and robustness of response taken. The finding is not too surprising given the skew in the data towards the United States as a target country. However, the effect is not statistically significant when controlling for the effects of other variables in the model, with large errors and wide confidence intervals. It remains an open question whether the United States' diplomatic responses are a result of its economic resources.

The strongest correlation in this analysis is between the number of allies that the target country has, and the robustness of its response to an OCO (0.507). As a country gains more allies, it tends to carry out harsher responses, including criminal charges, hack-backs, or sanctions, and this association is statistically significant (0.000). The United States has both a large number of allies globally and has often taken strong action against OCOs, according to the CFR data, so we cannot rule out a spurious relationship here. Nevertheless, it raises the possibility that a country like the United States is able to implement strong responses *because* of its international power and influence, as gauged here through alliances.

3.4 Findings & Limitations

Chosen cyber responses appear to be driven mostly by the international status of the target country. Alliances reflect and reinforce a country's global influence and power in the international system. Countries with more power are able to attract others into their sphere of influence.

That said, it is important to acknowledge the prominence of the United States in the data supporting this analysis. This is to be expected, given that it is the largest economy in the world, the most studied with respect to cyber security "as a great power" [12], and with a large numbers of international alliances, which makes it an attractive target. It is also in the top five countries most at risk of OCOs[11], and ranked in the top 5 of countries in terms of cyber security maturity [13]. Twenty-two of 25 responses coded as 'active' involved the United States. This analysis suggests that America's global influence might also play a role in explaining their willingness to punish cyber aggressions, and there is evidence that they are also helping other countries to repel OCOs [67, 75].

The analysis was carried out using the available data from the Cyber Operations Tracker, but we should be cautious about the conclusions we draw. As the authors of the data repository openly admit, the data is based on publicly known OCOs with a potential bias towards English speaking countries given the greater openness to reporting these events in the West. Further research is needed to understand how non-Western countries respond to OCOs.

Another limitation in the data is that it only captures responses to cyber-attacks that have been openly declared by the victim and misses responses that occur in secret. At this stage, we have little way of knowing the responses that have occurred unless these make their way into the public domain. This could help us interpret our finding that a high-status country such as the United States, is likely to engage in robust responses, given that powerful states are likely to be less deterred from openly confronting cyber aggressions. The data set probably under reports the way low status countries choose to respond to OCOs.

At a minimum, this analysis has helped describe the existing data on how states have responded in the past, and started a discussion of possible explanations. Having done so, we proceed to RQ2, to consider proposals for managing OCO threats.

4 RQ2: Proposed OCO Threat Management Possibilities

With a limited understanding of factors that trigger OCOs, we now consider advanced options for managing OCO threats. To judge these options, we will use Brantly's [8] deterrence dimensions, given that we are looking at this issue from a response perspective. Brantly claims that deterrence efforts have to have three core components: (1) having formulated the intention to protect the nation's cyberspace (credibility), (2) having the capabilities to implement that intention (capability), and (3) the communication of the intention and capability to a potential aggressor (communication).

4.1 A Cyber Geneva Convention

In 1949, the Geneva Conventions were ratified by 196 countries. These are international treaties that contain the most important rules limiting the barbarity of war. They protect people who do not take part in the fighting (civilians, medics, aid workers) and those who can no longer fight (wounded, sick and shipwrecked troops, and prisoners of war)[12].

Would a "Cyber" Geneva Convention be feasible? Brad Smith from Microsoft proposed exactly this in 2017 [64], with the idea of protecting citizens during peace times. In particular, signatories would have to agree not to target critical civilian electrical, economic and political infrastructures. This sounds sensible until you realise that there is no widely accepted definition of 'critical infrastructure' [44]. Jacobson [30] argues against Microsoft's proposal from a Danish perspective. He argues that such a digital convention would risk re-opening already concluded international agreements. Such an agreement might also serve to hamper existing cyber activities engaged in by smaller countries to protect themselves. Jacobson believes that involvement in the EU, NATO, the United Nations, as well as enhancing cooperation with the private sector, would enhance security in cyberspace better than a Cyber Geneva convention. Hollis [27] points to the fact that even those advocating for an international law for information operations are sceptical of a cyber 'Geneva Convention' given the volatility of technological innovation and development. This approach thus appears to fail on Brantly's *credibility* dimension.

4.2 Cyberspace as Ostrom's "Commons"

Elinor Ostrom was a political scientist at Indiana University who won a Nobel Prize for her research into how communities ought to co-operate to share resources. She referred to such shared resources as a "commons". Ostrom proposed eight principles for managing a commons [76]. Principle number six is: "*Use graduated sanctions for rule violators.*" Ostrom's 7^{th} principle specifies that resolution of disagreements between users of commons should be accessible and low-cost. This ensures that problems are solved rather than ignored and engenders inclusivity.

If Ostrom's 6^{th} and 7^{th} principles are not being respected by all Internet users, a cyber "tragedy of the commons" could exist, with some nations committing aggressions with impunity, essentially being bullies on the commons playground. Rankin *et al.* [54] explains this could end up destroying the very resource the world increasingly depends on.

At first glance, treating the Internet as a commons appears to be a viable approach to managing inter-country cyber aggressions, especially if these principles are enforced by an international body, such as the UN. However, we first have to consider whether cyberspace qualifies as a commons.

Kanuck [33] points out that other "commons" have been discovered by humans, not created by them. Kanuck argues that designating the Internet as a commons would require decisions to be made about how much, and which specific portions, of cyberspace would be governed according to these principles. It is likely that countries would consider their own essential infrastructures not to be part of the commons, but rather subject to individual property rights.

Fitzpatrick [23] argues that a sustainable sharing of "a commons" is only possible if reliable mechanisms are established to enforce compliance with agreed rules of usage. However, Kanuck [33] argues that the lack of transnational judicial cooperation makes any such enforced compliance infeasible. The other difficulty is that the reliable identification of legitimate users remains elusive. If it is not possible to identify people reliably, as passports do in the physical realm, it is hard to make people accountable for bad behaviours to sanction or exclude them. Applying such remediation to nation states is probably infeasible, and these are the infractions we are discussing here. This approach appears to fail on Brantly's *capability* dimension, making the idea of treating cyberspace as a commons infeasible.

4.3 Establishing Alliances

Based on our empirical investigation, even given the limitations, it seems that the way to be more powerful in cyberspace is to establish alliances with other countries, and sign treaties to formalise these. Accumulating allies to protect yourself is an age-old tactic. Cleopatra is said to have courted Mark Antony specifically because she saw his value as an ally[13]. The impact of the USA in swinging the outcome of both World Wars emphasised their value as an ally. Even today, many countries consider the USA a valuable ally [62], especially when a treaty is in place. On 19 July 2021, a senior USA administration stated: "*No one action can change China's behavior in cyberspace and neither can just one country acting on its own*" [65], confirming the power of international cooperation and collaboration.

Yet, the mere fact of having allies is not an absolute deterrent, when it comes to being targeted. Who the allies are, and their standing in the political sphere, also makes a difference. Clare [15, p.545] argues that "*allies only effectively deter challenges against those partners that are of a greater strategic importance*". Was this why the USA condemned the WannaCry ransomware OCO and joined the UK in attributing it to North Korea [7], even though the kill switch activated by the UK's Marcus Hutchins neutralised the threat before it compromised the USA's systems [45]? Perhaps it was because of the USA and UK's long standing Five Eyes Intelligence Alliance, or their history of being allies during recent conflicts.

This approach ensures that states benefit from the *capabilities* of their allies, and establishes their enhanced *credibility* in responding to OCOs. Our investigations suggest that this makes them able to respond to cyber aggressions, making the deterrence actions credible. The idea of forming alliances, if treaties exist, ensures that such alliances are salient, and *communicated* to others.

We need to reiterate, at this point, that our data was dominated by OCOs targeting the USA. The USA has many strong alliances. It might not be possible for other states to implement this strategy, nor is it guaranteed to give them the power to respond, perhaps in kind, to OCOs. Hence, this option is unlikely to be a globally feasible option.

4.4 The United Nations Approach

In 1945, after two of the biggest conflicts in the 20th century, the United Nations (UN) was created to maintain international peace and security, give humanitarian assistance to those in need, protect human rights, and uphold international law[14] [26]. At the time, no one could have anticipated cyber aggressions. The United Nations (UN) formulated eleven 'Cyber Norms' in response to the realisation that nation state cyber aggressions were occurring with increasing regularity [24].

Usually the action or response of the UN tends to be strategic, via treaties, conventions, written recommendations and consensus regarding specific issues [40]. The UN does actively engage "in the field". UN peacekeepers are a military peacekeeping group intervening in parts of the world where interventions are required. In the cyber context, the UN has been working actively e.g., by means of non-proliferation of mass weapons. This is because, should these weapons fall into the hands of malicious groups or private parties, the consequences could be dire and dangerous on a global level.

Considering Brantly's [8] mitigations in this respect, we can see the UN's *capability* as residing in its standing as an international body and recognition by the International Community. The UN's *credibility* [21] has been questioned a number of times, notably due to events and episodes that have occurred throughout its history that raised a number of critiques from different parties with reference to its functioning and management of crisis. Lastly, the UN has been quite active when it comes to its *communication*, putting in place a special department of communication [71]. Since its creation in 1946, a year after the UN's establishment, it has tackled disinformation and misinformation, specifically online [20].

4.5 Cyber Diplomacy

Torres and Riordan [69] explain that one of the UN's major roles is to establish norms of behaviour, which they have done. The second is to promote cyber diplomacy. Cyber diplomacy is defined as *"a set of diplomatic practices concerned with the broadly defined governance of cyberspace."* [53, p.2].

It seems sensible for governments to engage in diplomacy efforts, both cyber and traditional, to ensure that tense situations, perhaps post-OCO activity, do not escalate into open war. Conflicts have been prevented in the past when the leaders of the involved countries have met and resolved their differences to prevent escalation and eventual outright war. The Cuban missile crisis of 1962 is a case in point [32]. Kennedy and Khrushchev met and found a way to stand down their forces and a potentially devastating nuclear conflict was avoided. Diplomacy also seems indicated when an aggression has already been committed, such as SolarWinds, so that responses are measured and effective.

Levinson [38] argues that a law enforcement approach is unlikely to be an effective strategy in addressing nation state cyber aggressions, and this argument is echoed by O'Connell [51]. There are examples where the USA has preferred diplomacy to other approaches. Maness and Valeriano [41] determined that when China has engaged in attacking the United States, the United States has responded with diplomatic efforts. They have attempted to improve relations instead of responding by hacking back, for example.

With respect to Brantly's three dimensions [8], cyber diplomacy fulfills all of them. In 2016, the European Union wrote about the role of cyber diplomacy in building *capabilities* across the European Union. *Communication* is built into the definition of cyber diplomacy. *Credibility*, which encompasses governments' intention to act against the threat, and their formulation of strategies, is also built into the descriptions of cyber diplomacy and could be seen as the *raison d'être* for its existence. We now proceed to position cyber diplomacy within a strategic response to OCOs.

5 RQ3: Positioning Cyber Diplomacy

We now consider how a strategic approach could be formulated for managing the OCO threat. Instead of including only deterrence aspects, Carlin [10] suggests a 'Whole-of-Government Approach to National Security Cyber Threats'. Carlin recommends including the three D's: *deterrence*, *detection* and *disruption.* Cohen *et al.* [17] extend this with *defeat.* Based on the previous discussion, we extend this with a fifth dimension: *cyber diplomacy.*

Deterrence: Nye proposes a four-pronged deterrence approach: punishment, defence, entanglement and norms. Nye argues that this can "*reduce the likelihood of adverse acts causing harm in the cyber realm. They can complement one another in affecting actors' perception of the costs and benefits of particular actions*" [46, p.62]. Punishment is challenging in the cyber domain, due to the aforementioned attribution difficulty, compromising the ***credibility*** of the deterrence. Defence is related to implementing good cyber hygiene, signalling ***capability*** of deterrence efforts. Entanglement suggests creating dependencies between two states such that an attack would hurt the aggressor as well as the target. Finally, formulating and communicating norms imposes a reputational cost on aggressors, This fulfils the ***communication*** deterrence dimension.

Detection: Detection happened months, if not years, after the fact for the SolarWinds OCO [36] and for the Yahoo breach, which has also been attributed to unnamed "state sponsored actors" [19]. It might be that detection is being neglected in favour of deterrence. CISCO [14] recommends a number of ways to detect infiltration, including (1) identifying mysterious emails, (2) noting unusual password activity, (3) identifying suspicious pop-ups, and a (4) slower than usual network. These can be categorised either as anomaly detection (1-3) or performance monitoring (4).

Disruption: The third of Carlin's recommendations is disruption. This could include economic sanctions, coordination with other intelligence bodies such as the Five Eyes to share information and coordination with the private sector [10].

Defeat: Cohen *et al.* [17] explain that defeat refers to the efforts taken to reduce the number and severity of OCOs and to ensure that society can recover quickly from adverse cyber events. They advocate building resilience, which includes: implementing technical measures, human resource development, training exercises and, crucially, plans for recovering from the impact of OCOs that *do* succeed. Hence defeat includes the concept of *prevention*, as well as recovery.

Diplomacy: Cyber diplomacy has recently emerged as a viable mechanism to be used in this domain [1]. There is evidence that the USA has already started using diplomacy when engaging with particular countries [41].

5.1 The Five D's Framework:

In formulating the framework, we have to be cognisant of the cyber attack life cycle stages proposed by the USA's Cyber Threat Framework [48]: (1) preparation, (2) engagement, (3) presence, and (4) effect/consequence. The framework needs to include strategic responses for each of these phases.

Figure 3 brings everything together in a comprehensive framework describing how states can build a strategic response to the nation state cyber threat. The five D's (three from Carlin [10], one from Cohen *et al.*'s defeat and the fifth being cyber diplomacy) are mapped to Brantly's capability, credibility and communication dimensions [8].

This framework combines the preventive and reformative approaches to harm prevention [60]. We demonstrate how establishing alliances and the UN Norms would fit into these conceptualisations, as well as the formulation of plans for responses *pre-OCO*. Each of the "Five D" activities is expanded upon within their demarcated space in the diagram.

5.2 Countries' Cyber Security Strategies

Governments across the globe have formulated cyber security strategy documents[15] reflecting a growing understanding that the best way to manage cyber threats is to mount a strategic response, not a reactive tactical one. The existence of these policies demonstrates these countries' *credibility* in managing cyber threats. What is their strategy for dealing with OCOs?

Renaud *et al.* [55] analysed the cyber security strategy policies of the Five Eyes countries and China. Their analysis produced a list of government responsibilities mentioned by these countries' cyber strategy policies. All refer to the need to "*manage and mitigate cyber threats*", but do not provide a framework for specifically managing the OCO threat.

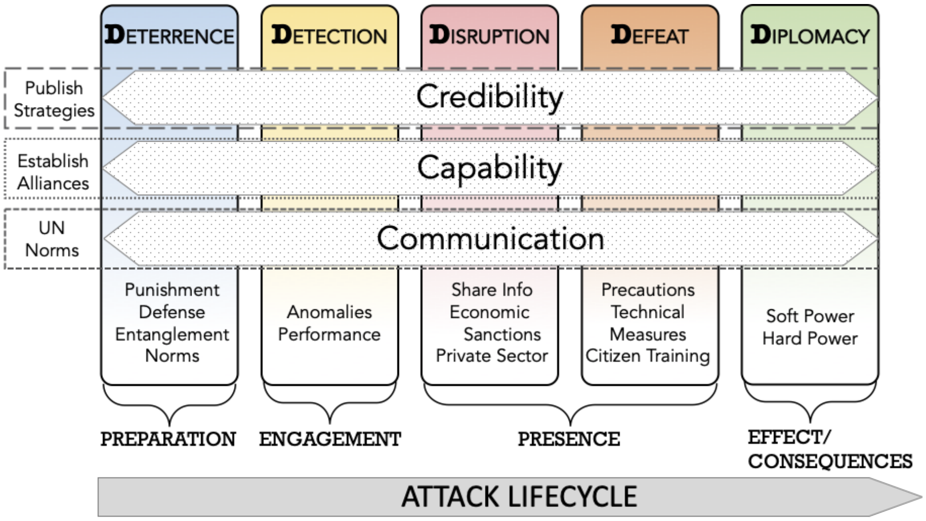

Fig. 3. The "Five D's" nation state cyber threat management framework

All also mention the responsibility to engage internationally and share information, which confirms the need to *communicate* with others and thereby to enhance their own *capabilities*. Interestingly, the USA alone mentions their responsibility to extradite cyber criminals, arguably a strong *deterrence* aspect. Detection is likely to be included in "*Coordinate reporting of vulnerabilities*" and "*Measure state of cyber security*". Disruption, defeat and diplomacy are not mentioned in the responsibility list. However, the Five Eyes countries are likely to be engaging in disruption and defeat activities, preferring not to mention these in their strategy documents, so as not to leak information that could benefit countries who might consider an OCO in the future.

It is also likely that these countries' governments do indeed have plans for dealing with OCOs that they have chosen not to share with the general public. Indeed, the USA announced that they had plans to prevent such an OCO on their 2020 election [49] and Cluley [16] reports that the USA is offering a reward for help in catching state-sponsored ransomware attackers. Moreover, the Biden administration just appointed their first National Cyber Director [28], with a remit to "*prepare the federal government's response to cyberattacks and cyber campaigns of **significant consequence***" (emphasis added by authors). This description suggests that a strategic response to OCO threats might well be part of the National Cyber Director's remit too.

6 Discussion & Conclusion

Cohen *et al.* [17] emphasise and highlight the importance of plans in coping with and offsetting the effects of OCOs. The "Five D's" framework's main contribution lies in its bringing all aspects of a strategic response into one framework, and pointing the way towards OCO mitigations. It enables a formulation of plans and implementation of measures *before* any OCOs occur. This paper reported on research carried out to answer the three research questions laid out in the introduction.

To answer **RQ1**, we identified and tested the influence of a number of factors that could play a role in triggering a robust response to an OCO. We discovered that diplomacy did not appear in reported responses to OCOs.

We then proceeded to advance a number of suggestions for managing the OCO threats. In addressing **RQ2**, only cyber diplomacy appears to satisfy all of Brantly's [8] dimensions.

Finally, to address **RQ3**, we propose a "Five D's" framework for a strategic response to managing the OCO threat. The framework is grounded in the research literature, and highlights the emerging and crucial role of cyber diplomacy in this space.

The factors we tested to answer RQ1 need to be augmented to provide a more comprehensive view of response influences. We hope that other researchers will help us to refine and improve the framework presented in Figure 3 so that it can become a useful resource for governments wanting to manage OCO threats to their own citizenry.

As future work, it would be worth investigating the impact of geopolitical factors on the cyber aggression realm, and especially the interplay of physical geography, pre-existing alliances and/or disputes due to physical proximity and emerging cyber capabilities. This investigation would seek to reveal the influence of physical proximity on cyber activities and aggressions. However, it must be acknowledged that the interconnectiveness of the world currently, might make geographical location less of an influential factor than it might have been two decades ago.

7 Limitations

As acknowledged in Section 3.4, our empirical investigation is USA centric, which means that we cannot easily generalise our findings. It is challenging to obtain better data sets but when these are published, we plan to run our analysis again on the more comprehensive data set to determine which factors significantly influence responses to OCOs.

Notes

[1] https://www.cyberarmscontrol.org/post/article-39-of-the-un-charter-cyber-as-a-threat-to-international-peace-and-security

[2] http://www.ieee-security.org/Cipher/Newsbriefs/1996/960723.EOonCIP.html

[3] https://fas.org/irp/offdocs/eo13010.htm

[4] https://legal.un.org/repertory/art51.shtml

[5] https://www.kaspersky.co.uk/resource-center/threats/ransomware-wannacry

[6] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

[7] https://www.cisecurity.org/solarwinds/

[8] https://microsites-live-backend.cfr.org/cyber-operations/search?keys=not+petya

[9] https://www.dailymail.co.uk/sciencetech/article-2637899/eBay-refused-admit-massive-cyber-attack-thought-customer-data-safe.html

[10] https://microsites-live-backend.cfr.org/cyber-operations

[11] https://nordvpn.com/cri/

[12] https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm

[13] https://www.scholaradvisor.com/essay-examples/cleopatra-relationships/

[14] https://www.un.org/en/about-us/history-of-the-un

[15] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

References

1. Attatfa, A., Renaud, K., De Paoli, S.: Cyber diplomacy: a systematic literature review. Procedia Computer Science **176**, 60–69 (2020)
2. Baldwin, D.A.: Power and international relations: A conceptual approach. In: Walter Carlsnaes, T.R., Simmons, B.A. (eds.) In Handbook of International Relations. Princeton University Press (2016)
3. Baram, G., Sommer, U.: Covert or not covert: national strategies during cyber conflict. In: 11th International Conference on Cyber Conflict (CyCon). vol. 900, pp. 1–16. IEEE (2019)
4. Barker, I.: Nation state attacks increase 100 percent in three years (2021), https://betanews.com/2021/04/08/nation-state-attacks-increase/
5. Barrinha, A., Renard, T.: Power and diplomacy in the post-liberal cyberspace. International Affairs **96**(3), 749–766 (2020)
6. Bayer, R.: Diplomatic Exchange Data set, v2006.1. (2006), https://correlatesofwar.org/data-sets/diplomatic-exchange
7. BBC: Cyber-attack: US and UK blame North Korea for WannaCry (2017), retrieved 1 May 2021 from: https://www.bbc.co.uk/news/world-us-canada-42407488
8. Brantly, A.F.: The cyber deterrence problem. In: 10th International Conference on Cyber Conflict (CyCon). pp. 31–54. IEEE (2018)
9. Brown, G.D.: Why Iran Won't Admit Stuxnet Was an Attack. Joint Force Quarterly **63**(4), 70–73 (2011)
10. Carlin, J.P.: Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. Harv. Nat'l Sec. J. **7**, 391 (2015)
11. Carpenter, P.: Cybersecurity And Nation-State Threats: What Businesses Need To Know (2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/04/16/cybersecurity-and-nation-state-threats-what-businesses-need-to-know/?sh=18d005817c21
12. Cavelty, M.D., Egloff, F.J.: Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. Swiss Political Science Review **27**(1), 139–149 (2021)
13. cipher: Which Country is #1 in Cybersecurity? (2021), retrieved 10 July 2021 from: https://cipher.com/blog/which-country-is-1-in-cybersecurity/

14. CISCO: Cyber Diplomacy in the European Union (2017), retrieved 2 May 2021 from: https://www.cisco.com/c/dam/m/en_ca/business-transformation/pdf/5-ways-to-detect-a-cyber-attack.pdf
15. Clare, J.: The deterrent value of democratic allies. International Studies Quarterly **57**(3), 545–555 (2013)
16. Cluley, G.: Us offers $10 million reward in hunt for state-sponsored ransomware attackers (2021), retrieved 17 July 2021 from: https://www.tripwire.com/state-of-security/security-data-protection/us-offers-10-million-reward-in-hunt-for-state-sponsored-ransomware-attackers/
17. Cohen, M., Freilich, C., Siboni, G.: Four Big "Ds" and a Little "r": A New Model for Cyber Defense. Cyber, Intelligence, and Security **1**(2), 21–36 (2017)
18. Coppinger, D.S.: Aggression in Cyberspace: Framing an Operational Response. Tech. rep., NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT (2010)
19. Cuthbertson, A.: Yahoo Data Breach Is 'Most Audacious Hack of All Time' (2016), retrieved 30 April 2021 from: https://uk.news.yahoo.com/yahoo-data-breach-most-audacious-163029811.html
20. Department of Global Communications: 5 ways the UN is fighting 'infodemic' of misinformation (2020), retrieved 2 May 2021 from: https://www.un.org/en/department-global-communications/
21. Earle, P.C.: Lockdowns Have Killed What's Left of the United Nations' Credibility (2020), retrieved 30 April 2021 from: https://www.aier.org/article/lockdowns-have-killed-whats-left-of-the-united-nations-credibility/
22. Fayi, S.Y.A.: What Petya/NotPetya ransomware is and what its remidiations are. In: Information Technology-New Generations, pp. 93–100. Springer (2018)
23. Fitzpatrick, D.: Evolution and chaos in property right systems: the third world tragedy of contested access. Yale LJ **115**, 996–1048 (2005)
24. GOV.UK: Implementing norms in cyberspace (2020), retrieved 30 April 2021 from: https://www.gov.uk/government/publications/implementing-norms-in-cyberspace
25. Hald, S.L., Pedersen, J.M.: An updated taxonomy for characterizing hackers according to their threat properties. In: 2012 14th International Conference on Advanced Communication Technology (ICACT). pp. 81–86. IEEE (2012)
26. Hanhimäki, J.M.: The United Nations: A very short introduction. Oxford University Press, Great Britain (2015)
27. Hollis, D.B.: Why states need an international law for information operations. Lewis & Clark L. Rev. **11**, 1023–1061 (2007)
28. Hunton Privacy Blog: White House to Nominate First National Cyber Director (2021), retrieved 18 July 2021 from: https://www.huntonprivacyblog.com/2021/04/14/white-house-to-nominate-first-national-cyber-director/
29. ID Agent: 10 Facts About Nation-State Cyberattacks That Will Keep You Up At Night (2020), https://www.idagent.com/blog/10-facts-about-nation-state-cyberattacks-that-will-keep-you-up-at-night/
30. Jacobsen, J.T.: En "digital Genèvekonvention" er ikke i Danmarks interesse. Internasjonal Politikk **76**(2), 73–88 (2018)
31. Jensen, L.: Maritime Cyber Security: It's all about the money (2021), retrieved 1 May 2021 from: https://improsec.com/cyber-blog/maritime-cyber-security-its-all-about-the-money
32. Jervis, R.: The Cuban Missile Crisis: what we know, how did it start, and how did it end. In: Scott, L., Hughes, R.G. (eds.) The Cuban Missile Crisis: A Critical Reappraisal (Cold War History). Taylor & Francis, Oxon, UK (2018)

33. Kanuck, S.: Sovereign discourse on cyber conflict under international law. TEx. L. REv. **88**, 1571–1597 (2009)
34. Kello, L.: The meaning of the cyber revolution: Perils to theory and statecraft. International Security **38**(2), 7–40 (2013)
35. Kostadinov, D.: The attribution problem in cyber attacks (2013), retrieved 30 April 2021 from: https://resources.infosecinstitute.com/topic/attribution-problem-in-cyber-attacks/
36. Lakshmanan, R.: Here's How SolarWinds Hackers Stayed Undetected for Long Enough (2021), retrieved 30 April 2021 from: https://thehackernews.com/2021/01/heres-how-solarwinds-hackers-stayed.html
37. Lee, E.: More Dependence on Internet Leads to More Cyberattacks Worldwide (2017), vOA News. Retrieved 8 May 2021 from: https://www.voanews.com/silicon-valley-technology/more-dependence-internet-leads-more-cyberattacks-worldwide
38. Levinson, M.: Why Law Enforcement Can't Stop Hackers (2011), retrieved 1 May 2021 from: https://www.cio.com/article/2402264/why-law-enforcement-can-t-stop-hackers.html
39. Lin, H.S.: Offensive cyber operations and the use of force. J. Nat'l Sec. L. & Pol'y **4**, 63–86 (2010)
40. Lustik, L.: Can the UN Prevent Cyber-Attacks? (2018), retrieved 1 May 2021 from https://thenewcontext.org/can-the-un-prevent-cyber-attacks/
41. Maness, R.C., Valeriano, B.: The impact of cyber conflict on international interactions. Armed Forces & Society **42**(2), 301–323 (2016)
42. Moret, E., Pawlak, P.: The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? (2017), european Union Institute for Security Studies (EUISS). Retrieved 8 May 2021 from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief24Cybersanctions.pdf
43. Murray, G.R., Albert, C.D., Davies, K., Griffith, C., Heslen, J., Hunter, L.Y., Jilani-Hyler, N., Ratan, S.: Toward creating a new research tool: Operationally defining cyberterrorism (2019), oSF Preprints
44. Newbill, C.M.: Defining Critical Infrastructure for a Global Application. Ind. J. Global Legal Stud. **26**, 761–780 (2019)
45. Newman, L.H.: How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack (2017), retrieved 1 May 2021 from: https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/
46. Nye Jr, J.S.: Deterrence and dissuasion in cyberspace. International Security **41**(3), 44–71 (2016)
47. Office of the Director of National Intelligence: NCSC Director Warns of Nation-State Cyber Threats to Law Firms in June 4 Remarks at ILTA LegalSEC Summit 2019 (2019), https://www.dni.gov/index.php/ncsc-newsroom/item/2002-ncsc-director-warns-of-nation-state-cyber-threats-to-law-firms-in-june-4-remarks-at-ilta-legalsec-summit-2019
48. Office of the Director of National Intelligence: Cyber Threat Framework (undated), https://www.odni.gov/index.php/cyber-threat-framework
49. O'Flaherty, K.: U.S. Government Confirms Plan To Defend 2020 Election Against Cyberattacks (2019), https://www.forbes.com/sites/kateoflahertyuk/2019/08/28/us-government-plan-to-halt-election-cyberattacks-misses-one-major-issue/?sh=7c1017de2041
50. Oved, M.C.: Journalist's phone hacked by new 'invisible' technique: All he had to do was visit one website. Any website. (2021), https://www.thestar.

com/news/canada/2020/06/21/journalists-phone-hacked-by-new-invisible-technique-all-he-had-to-do-was-visit-one-website-any-website.html

51. O'Connell, M.E.: Cyber security without cyber war. Journal of Conflict and Security Law **17**(2), 187–209 (2012)
52. Pomerleau, M.: State vs. non-state hackers: Different tactics, equal threat? (2015), https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx
53. Presidency: European Union: Cyber Diplomacy in the European Union (2019), retrieved 2 May 2021 from: https://eucyberdirect.eu/wp-content/uploads/2019/12/cd_booklet-final.pdf
54. Rankin, D.J., Bargum, K., Kokko, H.: The tragedy of the commons in evolutionary biology. Trends in Ecology & Evolution **22**(12), 643–651 (2007)
55. Renaud, K., Orgeron, C., Warkentin, M., French, P.E.: Cyber security responsibilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China. Public Administration Review **80**(4), 577–589 (2020)
56. Rid, T., Buchanan, B.: Attributing cyber attacks. Journal of Strategic Studies **38**(1-2), 4–37 (2015)
57. Rosenzweig, P.: Cyber warfare: how conflicts in cyberspace are challenging America and changing the world. ABC-CLIO (2013)
58. Schmitt, M.N. (ed.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, UK (2017)
59. Shackelford, S.J., Andres, R.B.: State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Geo. J. Int'l L. **42**, 971 (2010)
60. Sharma, U., Sharma, S.K.: Principles And Theory In Political Science Vol# 1. Atlantic Publishers & Dist, New Delhi, India (2000)
61. Sigholm, J., Larsson, E.: Determining the utility of cyber vulnerability implantation: The heartbleed bug as a cyber operation. In: 2014 IEEE Military Communications Conference. pp. 110–116. IEEE (2014)
62. Silver, L.: U.S. is seen as a top ally in many countries – but others view it as a threat (2019), retrieved 30 April 2021 from: https://www.pewresearch.org/fact-tank/2019/12/05/u-s-is-seen-as-a-top-ally-in-many-countries-but-others-view-it-as-a-threat/
63. Singer, E.O.: From reproductive rights to responsibilization: fashioning liberal subjects in Mexico City's new public sector abortion program. Medical Anthropology Quarterly **31**(4), 445–463 (2017)
64. Smith, B.: Keynote Address at the RSA Conference: The Need for a Digital Geneva Convention (2017), president and Chief Legal Officer, Microsoft
65. Starks, T.: US blames China for Microsoft hacking, ransomware attacks as part of global condemnation (2021), retrieved 19 July 2021 from: https://www.cyberscoop.com/china-microsoft-exchange-server-indictments-us-allies/
66. Terry, P.C.: "Don't Do as I Do"—The US Response to Russian and Chinese Cyber Espionage and Public International Law. German Law Journal **19**(3), 613–626 (2018)
67. The Associated Press: US, Estonia Partnered to Search Out Cyber Threat From Russia (2020), retrieved 2 May 2021 from https://www.usnews.com/news/politics/articles/2020-12-03/us-estonia-partnered-to-search-out-cyber-threat-from-russia
68. Tidy, J.: Solarwinds: Why the sunburst hack is so serious (2020), accessed 31 Dec 2020 from: https://www.bbc.com/news/technology-55321643

69. Torres, M., Riordan, S.: Policy Brief: The Cyber Diplomacy of Constructing Norms in Cyberspace (2020), retrieved 30 April 2021 from: https://www.ieeiweb.eu/wp-content/uploads/2020/10/T20_TF5_PB4_ok.pdf
70. Tsagourias, N.: Cyber attacks, self-defence and the problem of attribution. Journal of Conflict and Security Law **17**(2), 229–244 (2012)
71. United Nations: Telling the UN story in many languages, powered across platforms. (undated), retrieved 30 April 2021 from: https://www.un.org/en/department-global-communications/
72. Valeriano, B., Jensen, B.M., Maness, R.C.: Cyber strategy: The evolving character of power and coercion. Oxford University Press, New York, USA (2018)
73. Valeriano, B., Maness, R.C.: The dynamics of cyber conflict between rival antagonists, 2001–11. Journal of Peace Research **51**(3), 347–360 (2014)
74. Vavra, S.: NSA warns defense contractors to double check connections in light of Russian hacking (2021), retrieved 30 April 2021 from: https://www.cyberscoop.com/nsa-warns-defense-contractors-operational-technology-connections-russia-solarwinds/
75. Vercellone, C.: Ukraine is getting more help to build cyber capabilities (2020), retrieved 3 May 2021 from: https://www.fifthdomain.com/international/2020/03/04/ukraine-is-getting-more-help-to-build-cyber-capabilities/
76. Walljasper, J.: Elinor Ostrom's 8 Principles for Managing A Commons (2011), retrieved 22 April 2021 from: http://www.onthecommons.org/magazine/elinor-ostroms-8-principles-managing-commmons
77. Waltz, K.N.: Theory of international politics. Reading, Mass.: Addison-Wesley Pub. Co., (1979)