Cyber Operations in Peace and War: A Framework for Persistent Engagement

Brett van Niekerk
Durban University of Technology, South Africa
Security Insitute for Governance and Leadership in Africa, Stellenbosch University, South Africa

brettv@dut.ac.za

Abstract: During 1990s, the concept of information warfare (IW) and information operations (including cyber operations, psychological operations, and electronic warfare) could be conducted with varying intensity across all stages of peace and conflict. At that time, many of the concepts related to cyber operations were still hypothetical. Subsequently, conflicts and competition between states have demonstrated the capabilities and limitations of cyber operations. Research emerging in 2022 by multiple authors demonstrate the limitations and usage of offensive cyber operations and maintaining a sustainable military cyber capability, as well as proposing alternative models for conflict in cyberspace. Alongside this, there has been increased attention on the impact of ICTs on international security and the responsible behaviour of nation-states in cyberspace. There is still ambiguity and different perspectives on the application of international law in cyberspace. This uncertainty disrupts the original models of IW and warfare, which assumed clear distinctions amongst the conflict stages. Both the discourse of ICTs in international security and recent conflict necessitate a reconsideration of the decades-old view of IW in times of peace, war and the grey zone in between. This paper proposes a framework for the roles of cyber operations across the stages of conflict based on contemporary perspectives on the utility of cyber operations as well as practical examples. In rethinking the IW model, a multidisciplinary view is required, considering the technical, legal, social and international security perspectives.

Keywords: Cyber warfare, Influence operations, Information operations, Information warfare, Persistent engagement

1. Introduction

During the advent of information warfare (IW) and information operations in the 1990s, operations (including cyber operations and psychological operations) could be conducted to varying degrees through all stages of peace and conflict. While the scope of many IW operations was proposed for each of the conflict stages, at the time many of the concepts related to cyber operations were still hypothetical. Subsequently, the capabilities and limitations of cyber operations have been demonstrated (for example, in the Russo-Ukraine conflict). Research by Moore (2022), Smeets (2022), and Fischerkeller, Goldman and Harknett (2022) demonstrate the limitations and usage of offensive cyber operations and maintaining a sustainable military cyber capability.

In addition, there has been an increase in discussion on the impact of ICTs on international security, the relevance of international law to cyberspace, as well as responsible behaviour of nation-states in cyberspace. While there is agreement that international law applies to cyberspace and a set of norms have been established, there is still ambiguity on how international law is to be translated from the physical context to the virtual environment; for example, perspectives differ on what the threshold of an armed attack or an act of war in cyberspace is. This uncertainty disrupts the original models of IW, which assumed clear distinctions amongst the conflict stages. Furthermore, cyber diplomacy arising from the above-mentioned forums provides another mechanism of state power related to cyber operations, but also creates complexities.

Both the discourse of ICTs in international security and the Russo-Ukraine conflict necessitate a reconsideration of the decades-old view of IW in times of peace, war and competition. This paper proposes a framework for the roles of cyber operations across the stages of conflict based on contemporary perspectives on the utility of cyber operations, as well as lessons emerging from Ukraine and other practical examples. In rethinking the IW model, a multidisciplinary view is required, considering the technical, legal, social and international security perspectives.

Section 2 presents a background to facets of information warfare, the stages of conflict, and international cybersecurity. Cyber and disinformation operations are discussed in Section 3 with a view of demonstrating how they evolve over various stages of conflict. Section 4 provides the discussion and proposes an updated model for cyber operations across the stages of conflict; this is followed by the conclusion in Section 5.

2. Literature Review

This section provides the background to IW (Section 2.1), the stages of conflict (Section 2.2), and cyber diplomacy and cyber operations in international security (Section 2.3).

2.1 Information Warfare

Information warfare is a concept from the 1990s that incorporated a number of information activities aimed at affecting decision making and military operations (Waltz, 1998; Jones, Kovacich and Luzwick, 2002); the concept could be expanded into peacetime and was known as information operations. However, the usage of these terms has changed and tend to focus on the disinformation aspects, or occasionally purely the cyber component. Originally, information warfare included command and control warfare, military deception, economic information warfare, cyber operations, psychological operations, network-centric warfare, intelligence, and electronic warfare (Waltz, 1998; Jones, Kovacich and Luzwick, 2002). In addition, psychological operations have evolved with a strong cyber component in the form of influence operations due to the prevalence of social media. This evolution of mass disinformation and influence through the use of social media, supported by cyber operations, can be seen as a tool for diplomatic (or other) pressure on citizens and governments. Key to this is election interference, which has evolved due to these practices, and illustrated by Rid (2020). While Europe exhibits a number of examples of foreign influence operations, approximately 30 recorded disinformation operations in Africa are considered to originate externally, with half attributed to a single country (Africa Centre for Strategic Studies, 2022).

2.2 Stages of Conflict

Brahm (2003) lists the stages of conflict as (illustrated in Figure 1): latent conflict, conflict emergence, escalation, stalemate, de-escalation, settlement, and peacebuilding. However, Brahm (2003) notes that some stages may be repeated, and the transition between stages may not be smooth. For example, many conflicts may attempt to reach a settlement, only for an incident to occur and result in further escalation. The broader situation in the Middle East can be considered as one that oscillates amongst various stages; similarly, the situation in Ukraine de-escalated for a period, before returning to a full conflict scenario.

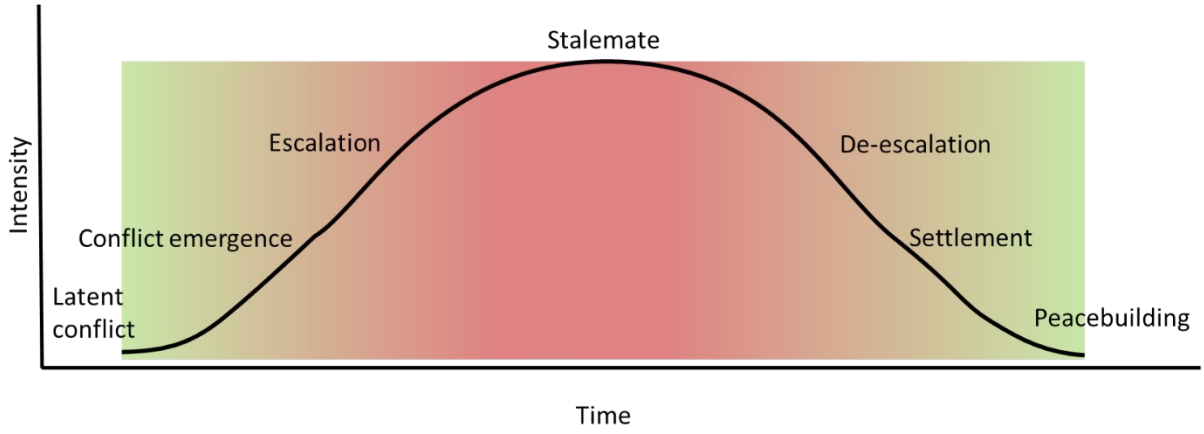

Figure 1: Stages of conflict, adapted from (Brahm, 2003)

Jones, Kovacich and Luzwick (2002) and Waltz (1998) present a similar six stage model for conflict, and indicate the prevalence of various IW activities for the stages, as is illustrated in Figure 2. The six stages are: considered as intelligence gathering, diplomatic pressure, economic pressure, military posturing, combat, and reconstruction.

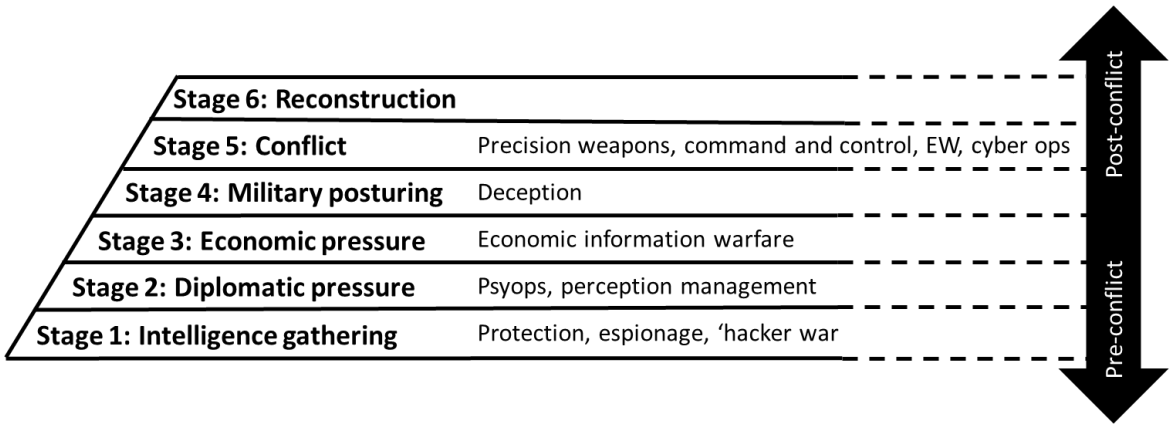

Figure 2: Stages of IW, adapted from Jones, Kovacich and Luzwick (2022) and Waltz (1998)

These models, however, are dated, and modern conflict appears to exhibit 'persistent' activity in the cyber domain. Therefore, the purpose of this paper is to propose a new alignment of cyber activities across conflict stages based on the concept of persistent engagement. For the purposes of this paper, the stages of conflict from both models need to be considered in conjunction with one another. The two models can be roughly aligned as shown in Table 1. It should be noted that diplomatic and economic pressure can be used as a tool for de-escalation, where pressure on the parties can result in them in seeking a settlement.

Table 1: Mapping of the two conflict models

Brahm (2003)	**Jones, Kovacich and Luzwick (2022) and Waltz (1998)**
Latent conflict	Intelligence gathering
Emergence	Diplomatic and economic pressure
Escalation	Military posturing
(Hurting) Stalemate	Conflict
De-Escalation	Diplomatic and economic pressure
Settlement/Resolution	Diplomatic and economic pressure
Post-Conflict Peacebuilding and Reconciliation	Reconstruction

2.3 Cyber Diplomacy and Cyber Operations in International Security

In attempt to address the potential impacts of cyber operations in an international security setting, a series of Group of Governmental Experts (GGEs) were established in 2004 under the auspices of the United Nations; a total of six GGEs were held, ending in 2021 (Schmitt, 2021). Of note, the 2015 GGE proposed non-voluntary norms to guide nations on responsible behaviour in cyberspace (UNGA, 2015). In addition to the GGE processes, Open Ended Working Groups (OEWGs) have been established as a more inclusive approach (Digital Watch, 2023). A number of initiatives have arisen in parallel to the UN processes, such as the Paris Call for Trust and Security in Cyberspace (2018) which proposed nine principles, and the Global Commission on the Stability of Cyberspace (2019), which proposes norms to protect the public core of the Internet. These initiatives are termed cyber diplomacy, which can be defined as "the means by which nations, groups, or individuals conduct their affairs in cyberspace, in ways to safeguard their interests and promote their political, economic, cultural or scientific relations, while maintaining peaceful relationships" (EU Cyber Diplomacy Toolbox, 2023). Cyber diplomacy helps guide state cyber operations and the implications for international security.

Healey (2021a) categorises four main frameworks for cyber operations in international relations research:

- Dyadic – cyber operations between specific organisations
- Strategic – cyber operations between nations through campaigns
- Asset – specific to technology (e.g. software and network)
- Systemic – system of systems related to the Internet

Research into the escalatory nature of cyber operations was conducted by Lonergan and Lonergan (2023) and Buchanan (2017), where Buchanan frames the escalatory nature within the context of a security dilemma in

cyberspace. Maness, Valeriano, Hedgecock, Macias, and Jensen (2023) consider the dyadic model of cyber incidents. Chesney and Smeets (2023) edited a book discussing cyber operations as primarily an intelligence competition. The concept of cyber persistence theory (persistent engagement) were discussed in Fischerkeller and Harknett (2019) and Fischerkeller, Goldman, and Harknett (2022).

Smeets (2022) discusses the challenges of establishing and maintaining an effective military cyber capability (as opposed to entering the cyber arena). Moore (2022) considers cases of a number of nations and their offensive cyber operations, and he notes that Iran recognises that achieving a top-tier status in the cyber domain is unlikely, therefore the focus is on being good enough to achieve objectives and signal that they are able to do so. However, Smeets (2022) indicates that a country with emerging capability that is determined to use it no matter what, may prove to be more dangerous than a state with developed capability but is restrained in its use.

Two posture statements released in 2023, one by the UK National Cyber Force (2023) and the other by General Nakasone (2023) of the US Cyber Command, provide insights into the operations conducted by the governmental cyber units. In both instances, the postures align to that of persistent engagement. However, both these nations are considered as having established capability and responsible legal guidance on their operations; other nations may have different capabilities and postures, and this could ultimately alter the dynamics thereby affecting the engagement in cyberspace (Healey, 2021a; Smeets, 2022).

Cyber persistence theory is based on the fact that the interconnectedness of nations through the Internet allows for competition in cyberspace, where cyber operations below the threshold of an armed attack can be conducted with limited risk of escalation. In some instances, the concept of forward defence may also be relevant, where a nation can disrupt on adversary's capability to conduct operations – in essence this is to defeat a cyber or influence operation as close to the source as possible. (Harknett, Fischerkeller & Goldman, 2023). Buchanan (2017) also considers the forward defence, but places this in the context of a security dilemma which results in escalation dynamics. A key component proposed by Fischerkeller and Harknett (2019) is that there is agreed competition. The current discussion in the cyber diplomacy circles can form part of this agreed competition even if it is implicit: national perspectives on international law in cyberspace are provided, which indicates the 'line' which could be considered escalatory.

3. Cyber Operations and Influence Operations Across the Stages of Conflict

This section provides perspectives on where and how cyber operations been employed during both periods of conflict and during times of peace.

3.1 The Early Days: Estonia and Georgia

In 2007 Estonia was subjected to distributed denial-of-service (DDoS) attacks in protest of a proposed relocation of a Soviet World War 2 memorial. Media, government websites and email, and banks were affected (Landler & Markoff, 2007; Rolski, 2007). This incident was the initial demonstration of the potential for cyber operations to be used for political and economic pressure.

In 2008, Russian forces intervened in the Georgia-South Ossetia conflict. Prior to this, DDoS attacks targeted the Georgia government and communications, resulting in a communications blackout. In addition, website defacements were used for propaganda and psychological operations (Coleman, 2008; Hart, 2008). This incident was a preview of how cyber operations could support military operations by creating a communications blackout. This was later refined for use in Ukraine, as describe in the next section.

3.2 Ukraine

Ukraine provides a particularly useful illustration of cyber operations across various stages of conflict. In 2014 popular protests ousted a pro-Russian government, which was followed shortly afterwards by the Russian occupation of Crimea, and an internal conflict in the East with pro-Russian separatists. In early 2022, Russian forces entered Ukraine. Cyber operations have played a part of this conflict; the CyberPeace Institute (2023) has recorded 2929 cyber operations by 122 unique threat actors associated with the Russo-Ukraine conflict between January 2021 and October 2023.

The incidents up to the end of 2022 are described in more detail by van Niekerk (2023), and a summary is provided below. In 2013 to 2014, cyber operations and online disinformation campaigns were conducted to support website defacements; DDoS attacks targeted regional organisations, but were prominent in attempting to disrupt Ukrainian communications prior to the Russian military incursion into Crimea, the Crimean referendum and the 2014 Ukrainian elections (also targeted by a disinformation campaign). Between the two

periods of physical operations, notable cyber operations included the disruption of the Ukrainian power grid in 2015 and 2016 by Russian advanced persistent threat (APT) groups, the NotPetya malware which is the costliest malware incident, a Ukrainian water treatment plant, and continued disinformation campaigns (van Niekerk, 2023). In addition, between 2014 and 2016 Ukrainian mobile phones were infected with spyware allowing Russian actors to track Ukrainian artillery units (van der Waag-Cowling, van Niekerk, & Ramluckan, 2022).

Immediately prior to the Russian incursion, an increase in disinformation campaigns was seen. The satellite provider Viasat was targeted to impact Ukrainian communications (similar to in Georgia and the Crimean annexation). During the early stages, notable cyber incidents included attempts by hacktivists to disrupt trains carrying Russian troops, and operations targeting Ukrainian power stations. A number of cyber operations targeting Russia were more symbolic, such as 'hack and leak' operations that released information about a nuclear power plant. What was unique during this period was the foreign assistance in the form of 'hunt forward' operations by US cyber command, and foreign corporations providing technical support to Ukraine. In addition, the Ukrainian president openly called for a volunteer cyber army to aid Ukraine (van Niekerk, 2023).

Subsequent reports indicate that there was a successful attempt on the Ukrainian power grid in October 2022, which coincided with missile strikes (Nelson, 2023), with ongoing attempts against the Ukrainian energy, government, and telecommunication sectors (CyberPeace Institute, 2023). The targeting appears to be more towards civilian infrastructure, to erode the national resilience and will, rather than to achieve specific military objectives.

The Ukrainian example demonstrates the used of influence operations to psychologically prepare the battlefield, and cyber operations to disrupt communications in the early stages of military action. Coordination between cyber operations and kinetic attacks appears to be evolving, however limited incidents appear to have the opportunity to directly impact on the battlefield, but rather targeting broader national and civilian resilience.

3.3 Iran

In 2010, the malware known as Stuxnet was discovered, and the prime target was determined to be the Iranian nuclear enrichment facility at Natanz. This cyber operation was significant in that it was the first recorded to affect industrial control systems and cause physical damage (Zetter, 2014); in addition, it demonstrated the strategic use of cyber operations n an attempt to maintain the status quo in terms of the balance of nuclear power.

Moore's (2022) opinion is that the Stuxnet incident made Iranian authorities realise the potential for cyber operations to further their asymmetric efforts at regional power projection; while they are not at the stage of a top-tier cyber power, their capabilities have evolved so that they are 'good enough' to achieve their objectives (Moore, 2022; Smeets, 2022). Notable cyber operations attributed to Iran (or proxy groups) include a wiper known as Shamoon targeting Saudi Aramco (Moore, 2022); the 2012 DDoS attacks against US banks and financial institutions either in protest to the movie *Innocence of Muslims* (Harris, 2014) or in response to US sanctions (Council on Foreign Relations, 2023); the targeting of a US dam (Brandom, 2016); the 2013 targeting of an unclassified US Marine Corps network and the 2014 targeting of US casino chains, Shamoon 2 and then in 2018 Shamoon 3 which targeted an Italian firm contracted to Saudi Aramco (Moore, 2022); and the targeting of the UK parliament in 2017 (The Telegraph, 2017). In July 2022, cyber operations targeted Albanian networks; these were attributed to Iran, resulting in Albania severing diplomatic ties with Iran in September of that year (Reuters, 2022). Iran was also accused, alongside Russia and China, in conducting influence operations and attempting to influence the 2020 US presidential elections; in 2017 Twitter reportedly closed 7000 fake accounts associated with Iranian influence operations (Timberg & Romm, 2019). Shample (2023) describes eight Iranian-linked APTs, all engaged with cyber-espionage against various regions and sectors.

Beyond the Stuxnet operation, the US alleged conducted cyber operations against Iranian air defence in response to the downing of a US drone in 2019 (BBC, 2019) and then again in response to an alleged Iranian attack on a Saudi Aramco oil facility (Ali & Stewart, 2019). In 2020, Iran allegedly attempted to target Israeli water infrastructure, to which Israel responded by targeting and disrupting the main Iranian port (Warrick & Nakashima, 2020; Times of Israel, 2020). In 2021, a hacktivist group targeted an Iranian steel plant, and then the petrol stations in 2022 (Bob, 2022).

The cyber operations both targeting and attributed to Iran demonstrate a range of objectives, from economic and diplomatic pressure, espionage, sabotage, to the possible disruption of air defence equipment. While none were conducted during the state of an official war, these incidents demonstrate cyber-operations across a range of conflict stages, with possible applications to a kinetic war. The cyber operations also demonstrate concepts

of proportional responses, where a cyber operation was conducted when a possible kinetic option was available, implying persistent engagement over escalation dynamics.

3.4 Election Interference

In 2016, foreign actors targeted the US presidential elections through a combination of disinformation and cyber operations, including a 'hack and leak' operation related to the Democratic National Committee emails. While these efforts were probably not directly successful; they did cast concern over election validity (amongst other scandals) and susceptibility (Office of the Director of National Intelligence, 2017).

As mentioned above, the 2014 Ukrainian elections were targeted by a cyber operation where the results were attempted to by altered, and this was supported by disinformation operations. However, the alteration was detected and unsuccessful, but the disinformation pre-empted the results and broadcast their altered voting counts (Clayton 2014).

Foreign election interference was experienced in at least five European countries from 2017 to 2018, including cyber operations and disinformation campaigns. Prior to the elections, European countries began with preparatory measures to defend the integrity of their election processes from interference (Brattberg & Maurer, 2018). Proposed measures to mitigate the interference operations include: international collaboration, public statements as deterrence, and legal measures (which can be considered related to cyber diplomacy); awareness, sensitisation, and training of the population, with responsible media engagement and empowerment; implement vulnerability assessments and incident response/contingency measures (Brattberg & Maurer, 2018).

In the run-up to the 2020 US presidential elections, four foreign states were attributed in running disinformation and/or cyber operations against the elections: Russia, China, Iran, North Korea (Timberg & Romm, 2019). Prior to election day in 2020, US Cyber Command collaborated with Microsoft to disrupt the TrickBot botnet to mitigate the threat of ransomware affection the elections (Vavra, 2020). In 2022, the US agencies proactively acted to disrupt foreign actors that allegedly intended to interfere with the US midterm elections (Nakasone, 2023). This is an additional possibility to mitigate election interference besides those measures proposed by Brattberg and Maurer. While the European measures were more aligned with traditional defensive mechanisms and diplomacy, the 2022 US approach is more aligned with persistent engagement.

3.5 Criminal Takedowns and Counter Terrorism

As is stated in the UK's Nation Cyber Force statement, they "may also use a combination of technical and information operations against hostile actors in a mutually supportive way, for example, to sow distrust in groups such as criminal gangs or terrorist cells" (NCF, 2023:13) and "Countering threats from terrorists, criminals and states using the internet to operate across borders in order to do harm in the UK and elsewhere" (NCF, 2023:20).

The statement by Nakasone (2023) also indicates that the US Cyber Command can "enable efforts" (Nakasone, 2023) by other government agencies and partners to disrupt online activities by cybercrime and extremist groups. The TrickBot example (Vavra, 2020) mentioned above is an example of such activities. However, Healey (2021b) suggests limitations on when an intelligence and military organisation such as Cyber Command should be used to disrupt criminal activity.

An interesting example is the 2019 Israeli response to persistent cyber operations by a sub-state actor, where they targeted the building that was identified as being used to conduct the operations with an airstrike (Borghard & Schneider, 2019). This was the first time a kinetic military response was invoked by cyber operations.

4. Cyber Espionage

Cyber espionage is probably the most common and persistent state-back from of cyber operations, which have been used against adversaries and allies alike. Harris (2014), Segal (2016) and Kaplan (2017) provide detailed histories of the evolution of cyber operations, and the prevalence of cyber espionage during conflict and peace is clear.

The next section provides a discussion on cyber operations during peace and war, and proposes an updated model for cyber operations across the various stages of conflict.

5. Discussion and Proposed Updated Model

From the examples described in Section 3, it can be seen there is a mixture of traditional defence strategies and persistent engagement strategies when considering cyber operations. Cyber diplomacy is an ongoing process through various forums. However, both the UK and US statements indicate that cyber operations can be employed to support foreign policy (NCF, 2023, Nakasone, 2023), implying that cyber operations themselves are a form of cyber diplomacy.

The Ukrainian example illustrates an escalation of influence operations and strategic cyber operations targeting civilian infrastructure. Some cases of strategic cyber operations were present between the two conflicts; however, these were limited and may have been experimental. Cyber espionage was present throughout the two periods of conflict and the intervening years. Foreign assistance in the form of forward defence proved to be a new evolution. By contrast, the Iranian example illustrates more posturing and targeting of civilian infrastructure as a form of economic and diplomatic pressure. The use of cyber operations in response to kinetic operations, and potentially impacting weapons systems have been reported but in limited cases. In general, proactive forward defence operations have been employed to disrupt foreign influence operations, possible election interference, cybercrime infrastructure and online terrorist activity. However, there should be careful consideration of when military or intelligence cyber capability is deployed against non-state actors, as discussed by Healey (2021b). Cyber espionage is ever present throughout the stages of conflict.

From the cyber operations considered above, 'conflict' in cyberspace does not necessarily follow distinct stages, but rather is a continuum with varying levels of intensity and types of operations. While cyber operations will peak in preparation for conflict or during actual conflict, there does appear to be an escalation on some operations during periods of diplomatic and economic competition. This may be to support foreign policy and diplomacy (i.e. signalling), of for possible experimentation to test cyber capabilities. Overall, while there is an increase in intensity during conflict, the majority of cyber operations do not appear to be specifically beneficial to kinetic battlefield operations, even though there have been coordinated cyber and kinetic operations. This view is supported in the analysis by van der Waag-Cowling, van Niekerk and Ramluckan (2022).

Cyber diplomacy is a continuous process, as is evidenced by the number of initiatives; during peace the intensity will be low to medium, but will increase along with growing competition and tensions. This is as a result of the increase in cyber operations alongside the increase in tension, necessitating an increase in the cyber diplomacy. Influence operations are also likely to be ever-present, with the intensity rising during times of competition (including elections as influence operations may overlap with election interference). There is a case where the intensity of influence operations may peak drastically during military posturing in order to stoke tensions or psychologically prepare populations for kinetic military operations. Cyber espionage is another ever-present form of cyber operations, and is of consistently medium to high intensity due to its utility in maintaining competition in economic, military, diplomatic, and research arenas, as well as in other crisis situations. Forward defence will only be present with low intensity during latent conflict, in defending against routine cyber espionage and he occasional cyber crime or cyber terrorist threat. This will peak drastically during military posturing to mitigate any preparatory offensive cyber operations, and may also form an aspect of foreign assistance, as was seen in Ukraine in 2022. Strategic operations will most likely only emerge during diplomatic or economic pressure, and will escalate as tensions increase, but sharply drop during de-escalation. Table 2 presents a proposed model for the varying intensities of various cyber operations across the traditional stages of conflict. The shaded areas for each of the five cyber operation types indicate the intensity, with one to five blocks available to represent a rating of one to five (maximum).

Table 2: Alignment of key themes to documents and proposed norms

Stage	Cyber diplomacy	Influence operations	Cyber espionage	Forward defence	Strategic operations
Latent conflict: Intelligence gathering					
Emergence: Diplomatic & economic pressure					
Escalation: Military posturing					

Stage	Cyber diplomacy	Influence operations	Cyber espionage	Forward defence	Strategic operations
Conflict & Stalemate					
De-Escalation: Diplomatic & economic pressure					
Settlement/Resolution: Diplomatic / economic pressure					
Post-Conflict Peacebuilding, Reconciliation & Reconstruction					

A challenge in this analysis is that there has not been a complete settlement or resolution phase after a kinetic conflict. A limitation of this perspective is that the capabilities of the nations are not explicitly considered. The examples described are all related to nations with developed capability. Conflict between nations with developing or limited capability may exhibit different uses of cyber operations.

6. Conclusion

The growing prevalence of cyber operations globally, and particularly amongst a set of nations, has necessitated a reconsideration of information warfare activities during various stages of conflict. An international relations model that has been proposed is one of persistent engagement. From the analysis of various examples, cyber operations can be seen to be conducted as a continuum across all stages of peace and conflict, with the intensity of various types of operations varying and generally peaking during (or immediately prior to) kinetic conflict. This supports the persistent engagement model for nations with an established cyber capability. A limitation of the study is that there is limited information on post-conflict peacebuilding, and on conflict between nations with developing cyber capabilities. Future work can expand on this study once a broader range of examples become available.

Acknowledgement

This work is based on the research supported in part by the National Research Foundation of South Africa (Grant Number 150720).

References

Africa Center for Strategic Studies. (2022) *Mapping Disinformation in Africa*, 26 April, [online], accessed 18 January 2023, https://africacenter.org/spotlight/mapping-disinformation-in-africa/

Ali, I., and Stewart, P. (2019). Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials, Reuters, 16 October, [online], accessed 18 December 2023, https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK/

BBC. (2019). US 'launched cyber-attack on Iran weapons systems', 23 June, [online], accessed 18 December 2023, https://www.bbc.com/news/world-us-canada-48735097

Bob, Y.J. (2022). Iran's steel industry halted by cyberattack, Jerusalem Post, 28 June 2022, [online], accessed 18 December 2023, https://www.jpost.com/middle-east/iran-news/article-710522

Borghard, E.D., and Schneider, J. (2019). Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal, *The Washington Post*, 9 May, [online], accessed 18 December 2023, https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/

Brahm, E. (2003) Conflict Stages, *Beyond Intractability*, September, [online], accessed 25 October 2023, https://www.beyondintractability.org/essay/conflict-stages

Brandom, R. (2016). How a DDoS campaign became an act of cyberwar, *The Verge*, 25 March, [online], accessed 18 December 2023, https://www.theverge.com/2016/3/24/11301876/ddos-iran-banks-dam-prosecution-indictment

Brattberg, E., and Maurer, T. (2018). Russian election interference: Europe's counter to fake news and cyber attacks, Carnegie Endowment for International Peace, 23 May, [online], accessed 18 December 2023, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

Buchanan, B. (2017) *The Cyber Security Dilemma: Hacking, Trust and Fear between Nations*. Oxford University Press: Oxford.

Chesney, R., and Smeets M. (2023). *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press: Washington, D.C.

Clayton, M. (2014). Ukraine election narrowly avoided 'wanton destruction' from hackers, *Christian Science Monitor*, 17 June, [online], accessed 8 November 2022, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoidedwanton-destruction-from-hackers

Coleman, K. (2008). Cyberwar 2.0 - Russia vs Georgia, DefenseTech.org, 13 August, [online], accessed 18 December 2023, https://www.military.com/defensetech/2008/08/13/cyber-war-2-0-russia-v-georgia

Council on Foreign Relations. (2023). Denial of service attacks against U.S. banks in 2012–2013, [online], accessed 18 December 2023, https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013

CyberPeace Institute. (2023). Cyber threats, [online], accessed 18 December 2023, https://cyberconflicts.cyberpeaceinstitute.org/threats

Digital Watch (2023). UN OEWG and GGE, Geneva Internet Platform, [online], accessed 12 January 2023, https://dig.watch/processes/un-gge

EU Cyber Diplomacy Toolbox. (2023). What is Cyber Diplomacy? Cyber Risk GmbH, [online], accessed 11 December 2023, https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

Fischerkeller, M.P., and Harknett, R.J. (2019). Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation, The Cyber Defense Review, Special Edition, 267-287.

Fischerkeller, M.P., Goldman, E.O., and Harknett, R.J. (2022). *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press: Oxford.

Global Commission on the Stability of Cyberspace. (2019). *Advancing Cyber Stability: Final Report*, November. Available at: https://hcss.nl/global-commission-on-the-stability-of-cyberspace-final-report/

Harknett, R.J., Fischerkeller, M.P., and Goldman, E.O. (2023). U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory, LawFare Blog, 5 April [online], accessed 14 December 2023 from https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory

Harris, S. (2014). *@War: The Rise of the Military-Internet Complex*, Houghton Mifflin Harcourt Publishing: New York

Hart, K. (2008). Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar, *The Washington Post*, August 14, p. D01. Available at https://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623_pf.html

Healey, J. (2021a). The Offense-Defence Balance in Cyberspace. Offensive Cyber Working Group, 20 April, [Youtube], accessed 2 December 2023 from https://www.youtube.com/live/XggIUBCwtTA?si=f2wWpMgDgphxpiHS

Healey, J. (2021b). When Should U.S. Cyber Command Take Down Criminal Botnets?, *Lawfare*, 26 April, [online], accessed 18 December 2023, https://www.lawfaremedia.org/article/when-should-us-cyber-command-take-down-criminal-botnets

Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002). *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. Auerbach Publications: Boca Raton, London & New York.

Kaplan, F. (2017). *Dark Territory: The Secret History of Cyber War*, Simon and Schuster: New York.

Landler, M., and Markoff, J. (2007). Digital Fears Emerge After Data Siege in Estonia. The New York Times Online, 29 May, [online], accessed 14 April 2010, http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1

Lonergan, E.D., and Lonergan, S.W. (2023). *Escalation Dynamics in Cyberspace*. Oxford University Press: Oxford.

Maness, R.C., Valeriano, B., Hedgecock, K., Macias, J., and Jensen B. (2023). Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000 to 2020, *Cyber Defense Review* 8(2), 65-89.

Moore, D. (2022). *Offensive Cyber Operations: Understanding Intangible Warfare*. Hurst Publishers: London.

Nakasone, P.M. (2023). 2023 Posture Statement of General Paul M. Nakasone, US Cyber Command, 7 March, [online], accessed 12 April 2023 from https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/

National Cyber Force [NCF]. (2023). The National Cyber Force: Responsible Cyber Power in Practice, Crown Copyright. Available at: https://www.gov.uk/government/publications/responsible-cyber-power-in-practice

Nelson, N. (2023). Sandworm Cyberattackers Down Ukrainian Power Grid During Missile Strikes, Dark Reading, 9 November, [online], accessed 7 December 2023, https://www.darkreading.com/ics-ot-security/sandworm-cyberattackers-ukrainian-power-grid-missile-strikes

Office of the Director of National Intelligence. (2017). Assessing Russian Activities and Intentions in Recent US Elections, Intelligence Community Assessment ICA_2017_01. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Paris Call for Trust and Security in Cyberspace. (2018) The 9 Principles, 12 November, [online], accessed 5 January 2023, https://pariscall.international/en/principles

Reuters. (2022). Albania cuts Iran ties over cyberattack, U.S. vows further action, 7 September 2022, accessed 18 December 2023, https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/

Rid, T. (2020) *Active Measures: The Secret History of Disinformation and Political Warfare*, New York: Farrar, Straus and Giroux.

Rolski, T. (2007). Estonia: Ground Zero for World's First Cyber War, *ABC News*, 17 May, [online], accessed 23 September 2009, http://abcnews.go.com/print?id=3184122

Schmitt, M. (2021). The Sixth United Nations GGE and International Law in Cyberspace, *Just Security*, 10 June, [online], accessed 27 January 2024, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Manoeuvre, and Manipulate in the Digital Age*, Public Affairs: New York.

Shample, S. (2023). Iranian APTs: An overview, *The Middle East Institute*, 10 February, [online], accessed 18 December 2023, https://www.mei.edu/publications/iranian-apts-overview

Smeets, M. (2022). *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*. Hurst Publishers: London.

The Telegraph. (2017). Iran blamed for cyberattack on Parliament that hit dozens of MPs, including Theresa May, 14 October, [online], accessed 18 December 2023, https://www.telegraph.co.uk/news/2017/10/13/iran-responsible-cyberattack-british-parliament/

Timberg, C., and Romm, T. (2019). It's not just the Russians anymore as Iranians and others turn up disinformation efforts ahead of 2020 vote, The Washington Post, 25 July, [online], accessed 18 December 2023, https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/

Times of Israel. (2020). Israel behind cyberattack that caused 'total disarray' at Iran port – report, 19 May, [online], accessed 18 December 2023, https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/

United Nations General Assembly. (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 17th Session, UN Doc A/70/174, 22 July.

Van der Waag-Cowling, N., van Niekerk, B., and Ramluckan, T. (2022). The Use and Potential of Cyber Weapons in Contemporary and Future Conflict, *Future Warfare and Technology: Issues and Strategies,* ed. RP Rajagopalan*, GP-ORF Series,* 97-106. Available at: https://www.orfonline.org/research/future-warfare-and-technologies/

Van Niekerk, B. (2023). The Evolution of Information Warfare in Ukraine: 2014 to 2022, *The Journal of Information Warfare* 22(1), 10-31.

Vavra, S. (2020). Cyber Command, Microsoft take action against TrickBot botnet before Election Day, CyberScoop, 12 October, [online], accessed 18 December 2023, https://cyberscoop.com/trickbot-takedown-cyber-command-microsoft/

Waltz, E. (1998*). Information Warfare: Principles and Operations*. Artech House: Boston & London.

Warrick, J. and Nakashima, E. (2020). Officials: Israel linked to a disruptive cyberattack on Iranian port facility, The Washington Post, 18 May, [online] accessed 18 December 2023, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon, *Wired*, 3 November, [online], accessed 18 December 2023, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/