Small State Acquisition of Offensive Cyberwarfare Capabilities: Towards Building an Analytical Framework

Daniel Hughes(✉) and Andrew Colarik

Massey University, Albany, New Zealand
Daniel.Hughes.1@uni.massey.ac.nz, A.M.Colarik@massey.ac.nz

Abstract. This paper examines the factors that motivate small states to acquire Offensive Cyberwarfare Capabilities (OCWC) and identifies the circumstances under which acquiring such capabilities is advantageous to a small state. First, the paper will offer a comprehensive analysis of the characteristics and limitations of OCWC, arguing that military conflicts are unlikely to be won solely by cyber weapons. Second, it analyses potential and likely uses of OCWC by small states and how these may advance political objectives, as explained by conceptual security models. Finally, the paper presents the first iteration of an analytic framework designed to provide a customized estimate of the desirability of OCWC acquisition for individual small states. The model is demonstrated by a case study on a member of the Five Eyes intelligence network and quintessential small state: New Zealand.

Keywords: Cyber · Warfare · Small states · Capabilities · Weapons · Acquisition · Framework · New Zealand

1 Introduction

This paper examines the factors that motivate small states to acquire Offensive Cyberwarfare Capabilities (OCWC) and identifies the circumstances under which acquisition would be beneficial. Literature to date has tended to focus on cybersecurity rather than cyberwarfare [1]. Accordingly, there is no analytical framework through which to consider whether small states should invest in OCWC. Questions regarding cyberweapon acquisition by small states will become increasingly important as they face difficult security investment choices due to the escalating costs of military platforms, uncertainties about the capabilities of cyberweapons, and the perception that OCWC are a low cost alternative to traditional military capabilities.

This paper first offers a comprehensive analysis of OCWC, based on a definition of cyberwarfare that, building on existing literature, underscores how cyberwarfare is the extension of policy via actions carried out through the increasingly militarized domain of cyberspace to create kinetic effects comparable to traditional military capabilities. This analysis is complemented by an examination of the balance of power between offensive and defensive cyberwarfare, the limitations of OCWC, and the concept of cyberpower, demonstrating that OCWC can neither win military conflicts unaided nor alter fundamental principles of warfare. Second, it analyses the likely uses of OCWC

M. Chau et al. (Eds.): PAISI 2016, LNCS 9650, pp. 166–179, 2016.
DOI: 10.1007/978-3-319-31863-9_12

by small states and the benefits and risks such use may generate. This analysis begins with a clarifying definition of the term 'small state', then continues with an examination of potential uses of OCWC: warfighting, coercion, deterrence, and defense diplomacy. This analysis is then refined by an examination of how these uses of OCWC can advance small state political objectives, as explained via multiple conceptual small state security models.

Lastly, this paper presents the first iteration of an analytic framework designed to recommend whether a particular small state should acquire OCWC. The framework begins by examining a small state's key quantitative and qualitative characteristics, along with its security and defense policies, military capabilities, and technical, financial and intelligence resources. This information is enriched by a consideration of the small state's 'cyber-dependence'– the degree to which its economy, military, and government rely on cyberspace, then a behavioral analysis of the state and its potential use of OCWC under conceptual small state security models. The sum of this analysis is evaluated against each category of potential OCWC use, resulting in predictive information regarding the utility of OCWC to the small state in question and a recommendation on the overall desirability of OCWC acquisition.

2 The Emergence and Characteristics of Offensive Cyberwarfare Capabilities

Cyberwarfare has become possible due to the advent of cyberspace, which despite its importance, does not have a commonly accepted definition. Building on academic [2], military [3] and policy [4] based definitions, this paper defines cyberspace as *a notional environment that consists of virtual and physical components. Its primary purpose is the transfer, storage and manipulation of information. It is a human-made domain and its existence relies on human-made objects and the energies of the electromagnetic spectrum*.

Cyberspace is the fifth domain (after land, sea, air, and space) to be militarized. These domains are interdependent; activities in one domain can create effects in and through one another [4]. Evidence of the escalating militarization of cyberspace can be seen in strategic documents, increasing investment in OCWC, and how cyber-attacks on US assets can now be considered to be of sufficient severity to warrant a traditional military response [5]. Despite this, cyberwarfare remains a contested term [6, 7]. In this paper, based on a synthesis of existing literature, cyberwarfare is defined as *an extension of policy via the military exploitation of cyberspace to create kinetic effects that approximate the effects of conventional weaponry. These effects either constitute a serious threat to a nation's security, or are conducted in response to a perceived threat against a nation's security* [6, 8, 9]. Accordingly, this paper defines Offensive Cyberwarfare Capabilities (OCWC) as *cyberweapons possessed by military or para-military organizations who have the will and expertise needed to use them to create military-grade kinetic effects*. The authors present these definitions in order to conceptualize this paper's use of OCWC.

Several commentators [4, 10] believe that cyberwarfare strongly favors OCWC over defensive cyber capabilities. Cyberspace, after all, is a target rich environment based on network structures that privilege ease of use over security. Attacks can be launched almost instantaneously; range and location are not limiting factors. There is rapid, growth in the number of networks and assets requiring protection and numerous vulnerabilities within critical infrastructure [11]. There are also considerable technical and legal difficulties that make accurate attribution of, and accurate and proportionate retaliation to, cyber-attacks a fraught process [12]. Finally there is the low cost of creating OCWC. Computer code is inexpensive to produce, and any cyberweapon released into the internet can be adapted to form the basis of new weapons [13].

The established modality of offensive cyber capabilities, however, are in question; other commentators [13, 14] are less certain of the dominance of OCWC. For example, cyber-dependence, the degree to which an attacker is dependent on cyberspace for functioning infrastructure, is crucial: increased cyber-dependence vis-a-vis an opponent will reduce the effectiveness of OCWC and increase vulnerability to retaliation. Uncertainty also rules in cyberwarfare, as shown by the 'dual use' [9] nature of cyberweapons - they can be captured, adapted and turned against their creators. Furthermore cyberattack vectors are rarely direct, and actions taken by states accidentally targeted are a significant risk. Equally important is the concept of 'escalation dominance' [15]. As shown by yet untested US policy, retaliation to a cyberattack need not be limited to cyberspace, but could instead be delivered by more traditional military means. Moreover, while the speed of a cyberattack may be near instantaneous, the preparation for large-scale, sophisticated cyberattacks is considerable. The Stuxnet attack, for example, required expansive espionage, industrial testing, sophisticated code, and clandestine delivery. Its creation required the resources of a technologically sophisticated nation; it was not built overnight [13].

The above illustrates an argument made by Rid & McBurney [16]: "Maximizing the destructive potential of a cyberweapon is likely to come with a double effect: it will significantly *increase* the resources, intelligence and time required to build and deploy such weapons – and more destructive potential will significantly decrease the number of targets, the risk of collateral damage and the coercive ability of cyberweapons." While this statement may seem in opposition to the low cost of creating cyberweapons; the costs it emphasizes are related to targeting and deploying weapons, not *creating* them. Advanced weapons must be targeted *before they are developed*. States must be certain about the objective and target of cyberweapons – they cannot be easily retargeted to meet unforeseen threats.

While OCWC have considerable destructive potential, they do have limitations. Ultimately they are pieces of computer code that rely on exploiting vulnerabilities caused by reliance on cyberspace [17]. They can attack vulnerable platforms and infrastructure by manipulating computer controlled safety systems, or act as a force multiplier to traditional military assets. These effects, however, are always secondary – cyberweapons cannot directly kill, injure, manipulate or destroy without a device to act through, nor can they occupy and control territory. As such, conflicts are unlikely to be won in the cyberspace alone.

Regardless of their limitations, a significant amount has been invested into the development of OCWC [4], and a significant number of states 'include cyberwarfare in their military planning and organization' [18], though reliable data on who possesses which cyberweapons and the capability of these weapons is highly classified [12]. This secrecy creates a broad spectrum of judgement concerning the threat posed by cyberweapons, which varies from conservative [19, 20], to moderate [13], to catastrophic [21]. These perspectives vary according to two factors: how much damage will accompany the compromise of cyber-dependent platforms and the extent to which major disruptions to state capabilities erode political will and can be exploited by traditional military force.

The growth of OCWC has seen some analysts [22, 23] explore the concept of 'cyberpower'. In the context of warfare, 'cyberpower' is only a new source of power in that it arises from a new military domain; it does not change the nature of power – the capacity to modify the behavior of others while preventing others from affecting one's own behavior [24]. Thus while it is important to identify what is new about cyberwarfare, it should be emphasized that cyberwarfare will not replace other domains of warfare, nor will it alter core principles of warfare, which remain subservient to political objectives.

3 Offensive Cyberwarfare Capabilities and Small States

Before analysis can begin on small state acquisition of OCWC, it is necessary to identify what the term 'small state' refers to. There has been no widely accepted definition of what constitutes a small state; disagreements have hindered consistent use of the term in literature [25, 26]. This has led to the rejection of the term [27] due to the relational and contextual nature upon which any classification of states into categories such as 'small', 'medium', or 'large' would rest. Modifying the work by Rickli [25], the characteristics that identify small states fall into three categories of measurement: *quantitative*, *qualitative-behavioral*, and *qualitative-self-identification*. *Quantitative* measures refer to quantifiable measures such as land area, population and Gross Domestic Product (GDP). *Qualitative-behavioral* measures concern the behavior of a state within the international system and *qualitative-self-identification* measures focus on how a state perceives its own identity.

For the purposes of this paper, the categorical tensions between quantitative, qualitative-behavioral, and qualitative-self-identification measures do not need to be resolved. Nor is a single, essential definition of 'small state' required. Instead, drawing on Wittgenstein's concept of 'family resemblance' [28], the concept of a 'small state' can be defined by possession of a sufficient number of overlapping characteristics – some quantitative, some qualitative-behavioral, and some qualitative-self-identification. No one category of measurement is essential to the definition of small state. Thus in order to analyze the acquisition of offensive-cyber-warfare-capabilities, the determination of state size can be made through a contextual and individualized examination of each state in question. For example the same quantitative measures of a state – population, geographic area, may indicate it should be considered as 'small'. However, an advanced economy, well developed military power, a history of exerting international influence

and self-identification as a regional power may mean that the state in question should be considered 'medium', not 'small'. This method of classification is representative of the information presented regarding the small state example that is presented in Sect. 4; it is a foundational aspect of the analytical framework offered in this paper.

To understand the benefits derived from small state acquisition of OCWC, it is necessary to understand how OCWC can be used. A non-exhaustive list of potential uses include *warfighting, coercion, deterrence,* and *defense diplomacy*. As OCWC are limited to secondary effects they have limited uses in warfighting. Their most prominent use is the disruption and manipulation of military Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities and the compromise of civilian support networks. Attacks on civilian infrastructure remain an option, and in the future attacks robotic military platforms are possible [29]. These tactics have a number of dependencies. First, the conflicting parties must have comparable military capabilities. Disrupting an opponent's C4ISR will be of little use if they still have the military superiority needed to achieve their objectives. Second, one state's disruption or destruction of another's cyber-infrastructure is only effective if they can defend their own assets, or have the capability to act without these assets with a minimal degradation in operational effectiveness. Third, states must have the resources required to deploy cyberweapons, which increase commensurate with the effectiveness of OCWC. Finally, cyberweapons usually rely on aggressive forward reconnaissance into networks of potential adversaries – the weapons should be positioned before conflict begins, which creates risks if an opponent discovers and traces a dormant cyberweapon. A further risk is the unpredictability of OCWC. Once unleashed the course of these weapons may 'be hard to predict, control, or contain' [14]. Unforeseen results may undermine relationships [22] or spread to unrelated states who then take retaliatory action.

Small state use of OCWC for coercion is similar to using them against state infrastructure in a warfighting scenario. It has the same dependencies regarding the relative size and cyber-dependence of an opponent, and shares the same risk regarding weapons acting in unforeseen ways. From a practical perspective, OCWC use for deterrence is little different from OCWC use for coercion. Both uses rely on the same aggressive forward reconnaissance of a potential opponent's network, so the difference between them becomes a matter of intent, which is difficult to prove. Another potential use of OCWC is defense diplomacy, which focuses on providing forces 'to dispel hostility, build and maintain trust and assist in the development of … armed forces' [30]. Activities include training, bilateral and multilateral personnel exchanges, and joint military exercises. This could be expanded to encompass cyber-exercises conducted by military cyber-specialists. Defence diplomacy can act as a deterrent, but is only effective if relevant military capabilities are credible [31].

Having identified potential uses of OCWC, it becomes necessary to also identify how they may advance the political objectives of small states. A small state's political objectives depend on its behavior and identity, both internally and in the international system, which can be hard to quantify. Some predicative analysis, however, is possible through the use of conceptual security models – especially if analysis is completed across multiple models. Burton's [1] literature synthesis argues that small state security policy

can be grouped under the conceptual models of *alliances, institutional cooperation*, and *identity and norms*. An alternative model emphasizes the two policy options of *collaborative influence* or *defensive autonomy* [25]. Synthesis of these approaches creates four models: alliances and collaborative influence, international cooperation and collaborative influence, identity and norms and collaborative influence, and identity and norms and defensive autonomy. Each model may have a greater or lesser amount of explanative power depending on the characteristics of the small state in question, but may provide substantive indicators for directional decisions.

The alliances and collaborative influence model presents small states with persuasive reasons to consider acquiring OCWC. This applies both to balancing behavior – joining an alliance against a threatening state, and bandwagoning, entering into an alliance with a threatening state [1]. The additional military resources provided by an alliance present greater opportunities for the exploitation of vulnerabilities caused by OCWC. In the event that a cyberweapon unwittingly targets a powerful third party, a small state may be less likely to be subjected to blowback if they are shielded by a strong alliance. Furthermore, OCWC may be a cost effective contribution to an alliance; a powerful state could even provide preferential OCWC procurement opportunities for a favored ally.

The institutional cooperation and collaborative influence model assumes that small states can exert influence by strengthening international organizations, encouraging cooperative approaches to security, and creating laws and norms to constrain powerful states [1]. Small states acting under this model will favor diplomatic and ideological methods of influence; and as such may be less likely to seek to acquire OCWC. Instead it is more probable that they will attempt to regulate OCWC in a manner similar to the restrictions on biological and chemical weapons, or by expanding current laws of international warfare to explicitly include cyberweapons.

As previously noted, the identity and norms model can be adapted to the pursuit of either collaborative-influence or defensive-autonomy. What is crucial to both variants of this model is the analysis of a small state's 'security identity', which grows from perceptions of 'past behavior and images and myths linked to it which have been internalized over long periods of time by the political elite and population of the state' [24]. This identity can be based around a number of disparate factors such as ongoing security threats, racial homogeneity, and parochialism. A state's security identity can lead it towards a collaborative security approach or a defensive, autonomous position, affecting the desirability of OCWC acquisition. It is this key divergence point combined with the above discussion that the authors present the acquisition framework in the next section.

4 Small State Acquisition of Offensive Cyberwarfare Capabilities: An Analytical Framework

The discussion and analysis offered in the previous sections suggests that a universally applicable recommendation on whether small states should acquire cyberweapons is not practical. The parameters of this decision depend too heavily on the behavior and identity of each particular small state and the scope of these attributes is too great to make universal pronouncements. Rather what is suggested is an analytical framework to

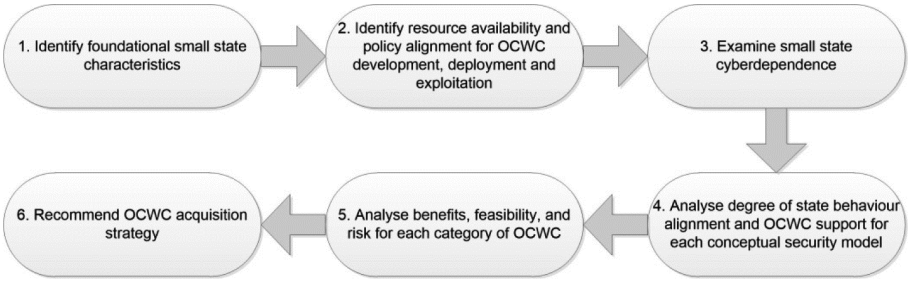

Fig. 1. OCWC acquisition framework

provide a customized evaluation of whether a particular small state should acquire OCWC. The first iteration of such a framework is provided below in Fig. 1.

Each step will be explained by a purpose statement, then demonstrated through a case study of New Zealand, chosen because it is both widely perceived as and self-identifies as a small state [32]. Ideally each step of the framework would be collaboratively completed by a group representing a variety of viewpoints from different government entities and academic specialties. There is the potential for a much more detailed evaluation than that presented, which has been condensed for brevity.

Step One – Identify foundational small state characteristics

Purpose: To identify key characteristics of the small state, under the categories of quantitative, qualitative-behavioral, and qualitative-identity. The starting point for determining these characteristics are the identifying measures that allow a state to be defined as 'small'.

Quantitative: New Zealand has a small population (approximately 4.5 million), a small GDP (approximately 197,000 million), and a small land area [33]. It is geographically isolated, bordering no other countries.

Qualitative-Behavioral: New Zealand practices an institutionally focused multilateral foreign policy [34]. It is a founding member of the United Nations and was elected to the Security Council for the 2015-2016 term after running on a platform of advocating for other small states. It participates in multiple alliances and takes a special interest in the security of the South Pacific [35].

Qualitative-Identity: New Zealand's self-identity emphasizes the values of fairness, independence, non-aggression, cooperation, and explicit acknowledgement of its status as a small state [32]. Its security identity is driven by a lack of perceived threat [36] that sometimes allows New Zealand to make security decisions based on principle rather than practicality. This was demonstrated by the banning of nuclear armed and powered ships within New Zealand waters, and its subsequent informal exclusion from aspects of the ANZUS Treaty. Despite reduced security, however, domestic opinion strongly supported the anti-nuclear policy [37], which, along with support for non-proliferation

and disarmament, has strengthened the pacifistic elements of New Zealand's national identity.

Step Two – Identify resource availability and policy alignment for OCWC development, deployment, and exploitation

Purpose: To identify: how OCWC use aligns with current security and defense policies; whether the small state has the military capabilities to exploit vulnerabilities caused by OCWC deployment (against both military and civilian targets); and whether the small state has the intelligence and technical resources needed to target, develop and deploy OCWC.

In key New Zealand defense documents [35, 36, 38], mentions to the cyber-domain primarily refer to defense against cyber-attacks, with only two references to the application of military force to cyberspace, and no mention of acquisition of OCWC. New Zealand's defense policy has focused on military contributions to a safe and secure New Zealand, a rules-based international order, and a sound global economy. As the likelihood of direct threats against NZ and its closest allies is low, there has been a focus on peacekeeping, interoperability, disaster relief, affordability, and maritime patrol. New Zealand's military is numerically small (11,500 personnel including reservists) with low funding (1.1 % of GDP). Military capabilities include deployable ground forces, logistic capabilities, C4ISR, and limited but credible combat capabilities [35]. Because of its current lack of offensive focus, the New Zealand military lacks the ability to exploit vulnerabilities caused by the successful use of OCWC.

New Zealand is a member of the 'Five Eyes' intelligence network, and as such has access to a much greater range of intelligence [1] than most small states, which can be used to increase its ability to target and deploy OCWC. It has a modern Signals Intelligence (SIGINT) capability, housed by the civilian Government Communications Security Bureau (GSCB), which also has responsibility for national cybersecurity. It most likely has the technical capability to adapt existing cyberweapons or develop new ones, particularly if aided by its allies. Due to fiscal constraints, however, any additional funding for OCWC will most likely have to come from the existing defense budget [35] and thus result in compromises to other capabilities.

Step Three – Examine small state cyberdependence

Purpose: To examine the small state's reliance on cyberspace for its military capabilities and critical infrastructure, and its relative cyberdependence when compared to potential military opponents.

New Zealand has moderate to high cyberdependence, with increasing reliance on online services and platforms by individuals, organizations, military forces, and other government entities. This dependence will likely increase over the next few years. For example, the acquisition of additional C4ISR capabilities and initiatives to increase military adoption of netcentric warfare principles [36] will create new vulnerabilities. New Zealand's cyberdependence is further increased by limited cybersecurity expertise [1]. New Zealand does not have obvious military opponents so its relative level of cyberdependence is difficult to calculate.

Step Four – Analyze degree of state behavior alignment and OCWC support for each conceptual security model

Purpose: To identify the extent to which the small state's behavior aligns with each security model (high, medium, or low) and the extent to which OCWC would support or detract from the effectiveness of state behavior under each security model.

Alliances and Collaborative Influence: New Zealand maintains a close military alliance with Australia and is a member of the Five Power Defence Arrangement. New Zealand has also recently signed cybersecurity agreements with NATO and the UK [1]. The alliances above have focused on security and mutual defense, rather than offensive capabilities. New Zealand does however, have a policy of complementing Australian defense capabilities [36]. This could be achieved through the acquisition of OCWC, so long as this was closely coordinated and integrated with the Australian military. *State Behavioral Alignment: Medium/High*

International Cooperation and Collaborative Influence: New Zealand usually pursues a multilateral foreign policy approach and is a member of multiple international organizations. It has a long history of championing disarmament and arms control [34], which conflicts with the acquisition of new categories of offensive weapons. *State Behavioral Alignment: High*

Identity and Norms and Collaborative Influence: With regard to collaboration, New Zealand's identity and norms strike a balance between practicality and principle. It wishes to advance what it regards as important values, such as human rights and the rule of law [32]. It however, still wishes to work in a constructive and practical manner. Procurement of OCWC is unlikely to advance this model. *State Behavioral Alignment: Medium*

Identity and Norms and Defensive Autonomy: Despite its multilateral behavior, NZ takes pride in maintaining independent views on major issues [32]. Its isolation and a lack of major threats has allowed it to retain a measure of autonomy in its defense policy and maintain a small military. Its independent and pacifistic nature suggest that OCWC acquisition could be controversial. *State Behavioral Alignment: Low/Medium*

Step Five – Analyze benefits, feasibility and risk for each category of OCWC

Purpose: To identify the benefits, feasibility, and risk of acquiring OCWC based on each category of potential use, as shown in Fig. 2, then to analyze this information against the degree of OCWC support for different security models in step four, as shown in Fig. 3. This results in a ranking of the benefits, feasibility, and risk under each combination of OCWC use and small state security model, as well as an overall recommendation for OCWC acquisition under each security model and OCWC use.

	Warfighting	Coercion	Deterrence	Defense Diplomacy
Benefits	Ability to complement military capabilities of allies Cost effective offensive capability	Limited coercive ability from OCWC	Limited deterrence from OCWC	Deterrence from demonstrating effective OCWC via defence diplomacy
Feasibility	Allies may provide favourable procurement opportunities Appropriate technical and intelligence resources exist	Appropriate technical and intelligence resources exist	Appropriate technical and intelligence resources exist	Appropriate technical and intelligence resources exist
Risks	Procurement may result in reduced funding for other military capabilities Domestic opposition to acquisition of new offensive weapons OCWC acquisition may reduce international reputation OCWC exploitation relies on allied forces High level of cyberdependence increases vulnerability to retaliation	Domestic opposition to acquisition of new offensive weapons Security identity not reconcilable with coercive military actions Procurement may result in reduced funding for other military capabilities OCWC acquisition may reduce international reputation High level of cyberdependence increases vulnerability to retaliation	Procurement may result in reduced funding for other military capabilities OCWC acquisition may reduce international reputation High level of cyberdependence increases vulnerability to retaliation Lack of identified threats reduces ability to target and develop deterrent OCWC	Procurement may result in reduced funding for other military capabilities OCWC acquisition may reduce international reputation High level of cyberdependence reduces deterrent effect

Fig. 2. OCWC benefits, feasibility and risk matrix

The authors accept that the rankings above are subjective in nature and require additional subject matter expertise and collaborative methods before they are relied upon by policy officials. They are offered in this spirit.

Step Six – Recommended OCWC acquisition strategy

Purpose: To summarise key findings, recommend if a small state should acquire OCWC, and identify the next steps advising how the framework's output should be used.

OCWC Acquisition Matrix: New Zealand						
Security Model	**BFR**	**Warfighting**	**Coercion**	**Deterrence**	**Defense Diplomacy**	**Overall**
Alliances and collaborative influence	Benefits	Medium	Low	Low	Medium	**Medium**
	Feasibility	Medium	Medium	Medium	Medium	**Medium**
	Risks	High	Very High	High	Low	**High**
	Recommendation	**Further Investigation**	**No**	**No**	**Further Investigation**	**Further Investigation**
International cooperation and collaborative influence	Benefits	Low	Low	Low	Medium	**Low**
	Feasibility	Medium	Medium	Medium	Medium	**Medium**
	Risks	High	High	High	Low	**High**
	Recommendation	**No**	**No**	**No**	**Further Investigation**	**No**
Identity and norms and collaborative influence	Benefits	Low	Low	Low	Medium	**Low**
	Feasibility	Medium	Medium	Medium	Medium	**Medium**
	Risks	High	High	High	Low	**High**
	Recommendation	**No**	**No**	**No**	**Further Investigation**	**No**
Identify and norms and defensive autonomy	Benefits	Low	Low	Low	Low	**Low**
	Feasibility	Medium	Medium	Medium	Medium	**Medium**
	Risks	High	High	High	Low	**Low**
	Recommendation	**No**	**No**	**No**	**No**	**No**

Fig. 3. OCWC acquisition matrix: New Zealand

Key Findings: New Zealand is unlikely to reap significant benefits from the acquisition of OCWC. This is due to its limited military capabilities, multilateral foreign approach, extensive participation in international organizations, and pacifistic security identity. The most likely factors to change this evaluation and increase the benefits of OCWC acquisition would be an increased focus on military alliances, the emergence of more obvious threats to New Zealand sovereignty, and a changing security identity.

Recommendation: It is recommended that New Zealand **does not acquire OCWC** at this time.

Next Steps: The output of this framework can be incorporated into relevant defense capability and policy documents. *If the framework had recommended the acquisition of OCWC*, then its output could be used to inform specific strategic, operational, and thus system requirements for OCWC. These capabilities could then be analysed under a standard return on investment business case model, in which a more detailed analysis of benefits, costs, and risks would allow an appropriate course of action to be decided in a transparent and fiscally responsible manner.

5 Conclusions

Recent analysis of cyberwarfare has been dominated by works focused on waning American hegemony, a rising China, Russian revanchism, and, growing cyber-bellicosity from rogue states and non-state actors. While not questioning the importance of these geopolitical trends, this paper shifts analysis to a relatively unexplored area – the factors that motivate a small state to acquire OCWC and the conditions under which acquisition would be beneficial. It offers a definition of cyberwarfare that focuses on its political and kinetic nature, complemented by analysis that challenges overestimation of OCWC. This is achieved through an exploration of the limitations of OCWC and the concept of cyber-power, arguing that OCWC can neither win military conflict unaided, nor alter principles of warfare. Second, it analyses both theoretical and likely uses of OCWC by small states. It argues that definitional tensions regarding the term 'small state' can be resolved by a definition that relies on the overlapping, qualitative and quantitative properties that are demonstrative of its identity and behavior. The paper then turns analyzes four categories of potential OCWC use, which are examined with regard to their potential to advance small state political objectives, as explained via multiple conceptual small state security models.

Having concluded that a universally applicable recommendation on whether small states should acquire cyberweapons is not possible, this paper instead presents an analytic framework designed to produce individualized recommendations on whether a particular small state should acquire OCWC. The framework has been demonstrated by a case study on a quintessential small state – New Zealand. It began with an analysis of the quantitative and qualitative characteristics that could be used to identify New Zealand as a 'small' state, followed by an examination of its security and defense policies, military capabilities, and technical, financial and intelligence resources. This was augmented by consideration of the extent of New Zealand's 'cyber-dependence' and a behavioral analysis of New Zealand and its potential uses of OCWC under small state security models. The results of this analysis have been assessed against each category of potential OCWC use, resulting in predictive information regarding the utility of OCWC and the overall desirability of OCWC acquisition. The framework demonstrates that New Zealand, with its limited military capabilities, absence of direct threats, institutionally focused foreign policy, and pacifistic security identity, is unlikely to benefit from the acquisition of OCWC at this time. This result, however, is unique to New Zealand; further small state examinations will enhance the OCWC acquisition framework offered as well as its utility in this decision process. The spectrum of small state behavior and identity is far-reaching; each small state must examine its own circumstances to determine whether the acquisition of OCWC will allow it to advance its own national security interests.

References

1. Burton, J.: Small states and cyber security: the case of New Zealand. Polit. Sci. (00323187), **65**(2), 216–238 (2013). doi:10.1177/0032318713508491
2. Mayer, M., Carpes, M., Knoblich, R.: (Introduction) The Global Politics of Science and Technology. Springer, Berlin (2014)

3. Vice Chairman of the Joint Chiefs of Staff: Joint Terminology for Cyberspace Operations (2011). http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf
4. Schrier, F.: On Cyberwarfare DCAF Working Paper No. 7 (2015). www.dcaf.ch/content/download/67316/…/OnCyberwarfare-Schreier.pdf
5. US Department of Defense. The DOD Cyberstrategy (2015). http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
6. Shakarian, P., Shakarian, J., Ruef, A.: Introduction to Cyberwarfare: A Multidisciplinary Approach. Syngress, Burlington (2013)
7. Theohary, C., Rollins, J.: Cyberwarfare and Cyberterrorism: In Brief. Congressional Research Service, Washington (2015). https://www.fas.org/sgp/crs/natsec/R43955.pdf
8. Colarik, A., Janczewski, L.: Developing a grand strategy for Cyber War. In: 2011 The International Conference on Information Assurance & Security (IAS), pp. 52–57 (2011). doi: 10.1109/ISIAS.2011.6122794
9. Parks, R.C., Duggan, D.P.: Principles of Cyberwarfare. IEEE Secur. Priv. Mag. **9**(5), 30 (2011). doi:10.1109/MSP.2011.138
10. Arquilla, J.: Twenty years of Cyberwar. J. Mil. Ethics **12**(1), 80–87 (2013)
11. Kiravuo, T., Tiilikanien, S., Sarela, M., Manner, J.: Peeking under the skirts of a nation: finding ics vulnerabilities in the critical digital infrastructure. In: Proceedings of the European Conference on e-Learning (2015)
12. Korns, S., Kastenburg, J.E.: Georgia's Cyber left hook. Parameters **38**(4), 60–76 (2009). Winter 08-09
13. Singer, P.W., Friedman, A.: Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, Oxford (2014)
14. Gompert, D. C., Libicki, M.: Waging cyber war the american way. Survival (00396338), **57**(4), 7–28 (2015). doi:10.1080/00396338.2015.1068551
15. Mahnken, T.: Cyberwar and Cyberwarfare. America's Cyber. Future **2**, 53–62 (2011). https://www.google.com.tw/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF8#q=Chapter+iV:+Cyberwar+and+Cyber+Warfare+By+Thomas+G.+Mahnken+citation
16. Rid, T., McBurney, P.: Cyber-Weapons. RUSI J. R. U. Serv. Inst. Def. Stud. **157**(1), 6 (2012). doi:10.1080/03071847.2012.664354
17. Carr, J.: The misunderstood acronym: why cyber weapons aren't WMD. Bull. At. Sci. **69**(5), 32 (2013). doi:10.1177/0096340213501373
18. Lewis, J., Timlin, K.: Cybersecurity and Cyberwarfare 2011 preliminary assessment of national doctrine and organization (2011). http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf
19. Gartzke, E.: The myth of cyberwar: bringing war in cyberspace back down to earth. Int. Secur. **2**, 41 (2013)
20. Rid, T.: Cyberwar and Peace. Foreign Aff. **92**(6), 77–87 (2013)
21. Clarke, R.D., Knake, R.K.: Cyber War. HarperCollins, New York (2010)
22. Nye, J.: Cyber Power (2010). http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf
23. Kuehl, D.T.: From Cyberspace to Cyberpower: Defining the Problem. Cyberpower and National Security, Washington (2009). http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf
24. Goetschel, L.: The foreign and security policy interests of small states in today's Europe. In: Goetschel, L. (ed.) Small States Inside and Outside the European Union, pp. 13–31. Kluwer Academic Publishers, Dordrecht (1998)

25. Rickli, J.: European small states' military policies after the Cold War: from territorial to niche strategies. Camb. Rev. Int. Aff. **21**(3), 307–325 (2008). doi:10.1080/09557570802253435
26. Sutton, P.: The concept of small states in the international political economy. Round Table **100**(413), 141–153 (2011)
27. Baehr, P.: Small states: a tool for analysis? World Polit. **27**, 456–466 (1975). doi: 10.2307/2010129
28. Wittgenstein, L., Anscombe, G.M.: Philosophical Investigations. The United Kingdom Basil Blackwell, Oxford (1958). c1953
29. Schutte, S.: Cooperation beats deterrence in Cyberwar. Peace Econ. Peace Sci. Public Policy **18**(3), 1–11 (2012). doi:10.1515/peps-2012-0006
30. Ministry of Defence Policy Papers Defence Diplomacy (1998). http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/BB03F0E7-1F85-4E7B-B7EB-4F0418152932/0/polpaper1_def_dip.pdf
31. Tan, A.T.: Punching above its weight: singapore's armed forces and its contribution to foreign policy. Def. Stud. **11**(4), 672–697 (2011)
32. McLay, J.: New Zealand and the United Nations: Small State, Big Challenge, August 2013. http://www.nzunsc.govt.nz/docs/Jim-McLay-speech-Small-State-Big%20Challenge-Aug-13.pdf
33. Statistics New Zealand, (n.d.): Index of key New Zealand Statistics. http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/index-key-statistics.aspx#
34. Ministry of foreign affairs and trade. Foreign Relations, March 2014. http://mfat.govt.nz/Foreign-Relations/index.php
35. New Zealand Defence Force. Defence Capability Plan (2014). http://www.nzdf.mil.nz/downloads/pdf/public-docs/2014/2014-defence-capability-plan.pdf
36. New Zealand Defence Force. Defence White Paper 2010 (2010). http://www.nzdf.mil.nz/downloads/pdf/public-docs/2010/defence_white_paper_2010.pdf
37. Reitzig, A.: In defiance of nuclear deterrence: anti-nuclear New Zealand after two decades. Med. Conflict Surv. **22**(02), 132–144 (2006). doi:10.1080/13623690600621112
38. New Zealand Defence Force. New Zealand Defence Force Doctrine (2012). http://www.nzdf.mil.nz/downloads/pdf/public-docs/2012/nzddp_d_3rd_ed.pdf