SSANSE
SMALL STATES AND THE NEW SECURITY ENVIRONMENT

RESEARCH PROJECT
POLICY BRIEFS

NEW ZEALAND'S AGENDA AT THE UN AND OTHER INTERNATIONAL ORGANISATIONS: INTERNATIONAL GOVERNANCE OF CYBERSPACE

Dr Joe Burton | University of Waikato | joe.burton@waikato.ac.nz

Policy brief no. 3 | June 3, 2017

Presented at the conference: 'Small States and the Changing Global Order: New Zealand Faces the Future' at University of Canterbury, Christchurch, New Zealand, 3-4 June 2017

The growing instability caused by cyber-attacks by state and non-state actors, including recent efforts to subvert democratic processes, demonstrates the need for a new approach to internet governance at the UN and a pressing need for an international treaty to govern cyberspace.

Key findings

- New Zealand has an opportunity to build on its recent efforts at the UN in advocating on issues that have resonance to small states in a changing security environment, but needs to prioritise issues on which it can build traction and support.
- Cyber security has climbed the ladder of importance in international security in recent years, and ongoing use of offensive cyber attacks to subvert, survey and attack foreign computer systems present a serious threat to international peace and stability.
- While there are some obstacles to international governance on cyber security issues, a cyber security treaty which seeks to address the proliferation of cyber weapons, a commitment to prohibit their use, and efforts to reign in mass surveillance is achievable if sustained advocacy on the issue takes place.

Executive summary

New Zealand's role at the United Nation has been a prominent one in recent years, with a period of service on the UN Security Council between 2014 and 2016, and following Helen Clark's tenure as the Director of the UNDP and high profile but ultimately unsuccessful bid for the position of United Nations Secretary General. A firm commitment to the UN as the ultimate arbiter of international peace and security has been a bedrock of New Zealand's foreign policy, stretching back to the formation of the organisation in San Francisco in 1945, and successive governments have sought to further New Zealand's many and varied interests through UN channels.

New Zealand's focus during its recent tenure on the Security Council was twofold: to reform the Security Council itself, and to try to positively influence the Israel Palestine peace process. Despite sustained efforts on both of these fronts, and despite a historic Security Council ruling on the status

NATO OTAN
This project is supported by: The NATO Science for Peace and Security Programme

of Israeli settlements, there has been little substantive change on either of these issues. On the latter issue, there has been some domestic discord too, with the new Foreign Minister Gerry Brownlee suggesting the Security Council resolution passed last December had been "premature" and should not have been proposed without the support of Israel.

As we move into a new period of arguably heightened geopolitical tension between the 'great powers', and the permanent five members of the security in particular, how should New Zealand reformulate its approach to the UN? What issues should be the focus of New Zealand's UN diplomacy, and how can these efforts be emulated in New Zealand's other engagements with international organisations, such as ASEAN, NATO, the EU, and other regional actors?

What is the problem?

One issue in need of urgent attention within the UN system (and other international organisations) is the growing misuse of the internet by state and non-state actors, and the heighted tensions stemming from cyber attacks that are taking place on a global scale and which are increasing in frequency and sophistication. Dozens of states have well-developed offensive cyber attacks capabilities, and even small countries like New Zealand are recognising that militaries need to have at least a defensive role and capabilities to enhance their cyber security.

The recent wannacry virus ransomware attack demonstrates that 'cyber weapons' are being developed by national security agencies, that those capabilities are being targeted for theft by state actors and non-state actors, and that the proliferation of these kinds of malicious software devices can cause widespread damage – the wannacry virus has spread to over 150 countries, and has likely caused billions of dollars of direct and indirect damages. This latest example of the adverse impacts of cyber attacks is part of a pattern of activity stretching back at least a decade, with a cyber barrage against Estonia (a similarly small highly networked nation to New Zealand) in 2007 by Russia-based hackers, use of cyber attacks by Russia in the Russia Georgia war in 2008, revelations about the US and Israeli use of the Stuxnet virus against the Iranian nuclear programme in 2010, the Shamoon virus used against energy company Saudi Aramco by Iran in 2012, which led to 3000 hard drivess being wiped of data, and the Sony hack in 2014, allegedly by North Korean hackers, which threatened to escalate into a major crisis between the US and North Korea.

What should be done?

To mitigate these kinds of malicious activities, The New Zealand government should adopt a policy to advocate for a new UN treaty on the International Governance of Cyberspace. The treaty would: include prohibitions on the use of weaponised malicious software inside and outside of armed conflict and against civilian infrastructure; mandate that all signatories cooperate in bringing those responsible for major cyber attacks to justice; outlaw cyber espionage and mass surveillance of the internet by government and private actors; mandate international cooperation on bringing cyber criminals to account.

Analysis

There are various barriers and obstacles to a UN treaty level commitment to governing cyberspace and these should be clearly acknowledged at the outset.

The first is that there has been some scepticism among our international partners, most notably the US and in Europe, to a UN role in governing cyberspace. Until the present time, the attitude has been that cyberspace should be a free and open platform for communications and trade and that international regulation through the UN system is undesirable.

Another issue is that China and Russia, along with other countries, have advocated for greater degrees of state control of the internet, reserving the rights of governments to maintain censorship and controls over content. This basic governance divide will not be easy to overcome and can be seen in recent Russian and Chinese efforts to advocate for the adoption of a 'code of conduct' on cyber security through UN channels.

A third issue is that we have not reached the full potential of internet technologies yet, and the rapid evolution of cyber capabilities risks making any binding legal agreement redundant in a short time horizon.

Additionally, unlike in the nuclear domain, verification of cyber weapons is much more difficult to achieve. The ease with which malicious software can be hidden, the corresponding difficulty and establishing any kind of inspection and verification regime, and the ongoing strategic and military utility of offensive cyber capabilities all present obstacles to widespread acceptance of the need for a UN level cyber treaty.

Despite these challenges (and there are many others) the vulnerability of all nations to cyber-attacks, the growing dangers of cyber escalation, and the very substantive platforms that have been established already (through the EU Cyber Security Strategy, Budapest Convention, and UN Experts Working Group on Cyber Security Norms of Behaviour) presents a moment of opportunity to progress these issues at the UN and other organisations.

Why does this matter to NZ?

New Zealand is not immune to cyber-attacks and has itself experienced a growing pattern of malicious attacks against its digital infrastructure, critical service providers and government ministries. This has been widely documented, including by our own intelligence agencies. As a highly networked nation, increasingly reliant on online trade in goods and services for economic growth, New Zealand is in a vulnerable position. At the same time, there is a very real opportunity for New Zealand in this area of policy. Joseph Nye has recognised that smaller actors, including small states, can exercise greater influence on cyber security issues, and this should apply to cyber security governance too. Given our historic commitment to peace and disarmament, our previous role in advocating nuclear non-proliferation treaties, and our seemingly independent reputation, New Zealand is well placed for international advocacy on these issues through the UN and other organisations, most notably at ASEAN and through the ASEAN Regional Forum, which has made cyber security a high priority in recent years. New Zealand's own cyber security strategy recognises the importance of international engagement and cooperation on cyber security but could be more ambitious.

Policy advice points

- In revising New Zealand's cyber security strategy, the New Zealand government should make a firm commitment to the introduction of a UN level cyber security treaty to address the issue outlined in this briefing paper.
- New Zealand diplomats at the UN and other organisations should be directed to make international cyber security governance a priority in their interactions.
- New Zealand should set up an experts working group of its own to examine how New Zealand can best advocate and achieve a UN level agreement on cyber security and overcome some of the obstacles involved.

Conclusion

Cyberspace is a vehicle for economic growth, for communication, for dialogue, for democracy and transparency. But in recent years the darker side of the world-wide web has been clearly in evidence. If sustained action is not taken now, it is no exaggeration to suggest that the internet itself, at least in its existing form, could be under threat.

NATO OTAN

This project is supported by:

The NATO Science for Peace and Security Programme