RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No. 052 – 26 September 2022

BYTES FROM UKRAINE
Cyber Warfare and Cyber Tantrums

In the opening days of the Ukraine conflict, some anticipated that it would become the first war fought largely in cyberspace. Six months on, ***EUGENE E. G. TAN*** *argues that cyberattacks have played only a supportive role to Russia's conventional war operations. However, he notes that cyberattacks have been used by various actors to signal displeasure to parties that have shown sympathy for Ukraine. He warns that states and their societies are increasingly likely to face such "cyber tantrums" by actors aggrieved by their policies.*

Cyber war may not take place … but cyber tantrums will. *Photo by AltumCode on Unsplash, modified.*

Six months have passed since Ukraine was invaded. While the effects of the physical conflict are devastating for Ukraine, the war being fought in cyberspace dims in comparison, contrary to widespread expectation. The Ukraine war provides an interesting test case for the role of cyberattacks in warfare, as well as for the corollary

of cyberattacks on states that are not party to a particular war but sympathetic to its victims. However, cyberattacks are not always readily attributable to state actors, making it difficult to link them to a clear campaign on the part of any given state.

What lessons can we draw from recent cyberattacks? And, what do the increasing number of threatened or realised cyberattacks mean for states and societies at large?

Role of Cyberattacks in War

First, while cyberattacks have undoubtedly been used in times of war in recent years, their scale and impact fall well below those of the use of armed force. In his seminal piece "Cyber War Will Not Take Place", Thomas Rid argues that cyberattacks are fundamentally a more sophisticated way of conducting subversion, espionage, and sabotage; cyberattacks on their own do not carry the same lethality that conventional warfare does and therefore do not constitute acts of war in their own right. Rid does acknowledge that in extreme circumstances a cyberattack in itself may constitute an act of war, but only when it causes massive destruction and damage. Nadia Kostyuk and Erik Gartzke agree with Rid in saying that cyber operations are most effective in pursuing informational goals. They go further by noting that cyberattacks are not pure substitutes for armed conflict but are likely to increasingly displace conventional conflict in future.

The above being said, in 2016, the North Atlantic Treaty Organization (NATO) formally recognised cyberspace as "a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea", making it clear that cyberattacks are considered a part of war — if not constituting its entirety.

The Ukraine war has demonstrated these principles quite clearly. Cyberattacks have been used in a limited way in support of conventional war operations but they have neither surpassed the use of force threshold, nor have they yet had lethal consequences.

Disclosures by Microsoft show that as part of its preparations for war Russia had deployed cyberattacks on critical infrastructure in Ukraine to disrupt Ukrainian communications. While most of these cyberattacks were thwarted by the Ukrainians, the Russians were successful in disrupting some critical services for a few days, including telecommunication services provided by ViaSat's KA-SAT satellite network.

It is also worth remembering that hostile cyberattacks on Ukraine are not new; they have been taking place on and off since the Russian annexation of Crimea and parts of the Donbas in 2014. The hacking of the Ukrainian power grid in the depths of the winter of 2015–2016 was particularly notorious and could potentially have been considered tantamount to an armed attack, had there been fatalities.

These incidents probably served as impetus for Ukraine to strengthen its cyber defences against external aggression, which should be seen as a positive example of how good cyber defences can prevent the disruption of services.

The relative lack of lethal and destructive effects means that it would be a gross overreaction to label cyberattacks in general as acts of war in themselves. This is

especially the case when cyberattacks occur as one-off events without other physical manifestations of war, such as the devastation of infrastructure and loss of life.

Cyberattacks or Cyber Tantrums?

The second lesson that we might draw from the recent and mounting cyber threat — which should be more worrying to states — is the rising number of cyberattacks that take place below the threshold of war, and the reasons why these are undertaken. Critical infrastructure, services, and data are susceptible to cyberattack, and such attacks are set to heighten in sophistication and frequency, even in peacetime or on countries that are not party to wars like those in Ukraine.

The Ukraine war has shown how societies at large have been on the receiving end of what could be called cyber tantrums, where attackers whose identities are unclear use cyberattacks to signal retaliatory discontent over a certain decision a country (or even an institution, business, or organisation in that country) has made.

Cyber tantrums may be targeted at various spheres: cultural, like the attempted cyberattack on the May 2022 Eurovision Song Contest held in Italy (which, perhaps uncoincidentally, was won by Ukraine); political, like the attack on multiple Lithuanian government websites for the country's decision to apply European Union sanctions against Russia for the Ukraine war; or even undertaken for personal reasons such as the religious, like the call for cyberattacks on the Singapore government in conjunction with an Indonesian preacher having being denied entry into the country.

Singapore, too, may well see cyberattacks for its decision to speak out against the war in Ukraine. Similarly, Singapore could be subject to future attack should another state (or state-sponsored actor, hacktivist, or opportunistic actor) take umbrage at its foreign policy or remarks made by senior officials. Singapore should be prepared for the likelihood of some of these cyberattacks getting past its cyber defences, and the authorities should prime the public for such disruptive measures.

Upholding a Rules-based Cyber Order

The third, and arguably the most important lesson that the war in Ukraine has taught the world is that there may be costs involved in standing up for global security. Cyber tantrums will become more commonplace as a greater number of geopolitical (and even ideological) flashpoints start coming to the fore, because cyberattacks are seen as low-risk, high-reward activities which have visible, albeit reversible, consequences. For example, a hacked power grid could greatly inconvenience a state by depriving it of critical services, although for the most part, power may be restored.

However, the risk of cyberattacks getting out of hand in times of war appears to be much lower than popularly thought, for it is generally recognised that cyberspace is governed by international law, as is the use of force and armed conflict. This principle was already agreed upon in 2013 by the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which two years later proposed 11 voluntary, non-binding norms of responsible state behaviour to guide state actions in cyberspace. The norms were re-endorsed by the UN General

Assembly as recently as September 2021, and again by delegates to the UN Open-ended Working Group on security relating to information and communications technologies at its third substantive session in July 2022.

The International Committee of the Red Cross argues that acts of cyber aggression in times of war should be covered under established international articles like the Law of Armed Conflict (or International Humanitarian Law). Hostile acts committed against Ukraine in cyberspace could therefore be considered part of the greater war on Ukraine. These could potentially include indiscriminate cyberattacks on healthcare facilities and civilian infrastructure.

States should therefore work towards developing wider adherence to norms and international law in cyberspace, in particular the 11 norms proposed by the 2015 UNGGE. There is scope for states to enact capacity- and confidence-building measures to develop a trusted and well-equipped system to jointly tackle cyber threats. These could involve supporting one another in developing cyber defence capacity, sharing intelligence on likely threats, and tackling cybercrime. It is only through international cooperation that states might reduce the reward or satisfaction gained by malicious cyber actors and make it harder for them to penetrate their systems.

This is not to say that errant states will not test the limits of the applicability of international law, especially if they can use proxies for deniability. The invasion of Ukraine is itself general proof that international law can be flouted. But it should be remembered that without the boundaries that international law has established, it would be difficult to even talk in terms of wrongdoing by states and other miscreants, much less pinpoint it.

The war in Ukraine has shown how even states that are not directly involved are not spared the effects of the war, albeit these occur on a much smaller and non-lethal scale. Cyber tantrums by states or non-state actors cannot be wished away, but they can be made less effective through the deepening of cooperation between states and other stakeholders. States might often be tempted to turn a blind eye to — or even encourage — cyber tantrums, because these fit their general purposes. This must end. The message that cyber tantrums are not to be condoned must be made clear to all stakeholders, if states desire stability and security in cyberspace in times of both war and peace.

Eugene E. G. TAN *is an Associate Research Fellow at the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies. He is currently working on capacity building measures and norm implementation for responsible state behaviour in cyberspace.*