CLEIMUN20

"Diplomacy in a Challenging Global Environment"

A Research Report

COMMITTEE: Disarmament and International Security Committee

QUESTION OF: State-Sponsored Cyber Attacks

AUTHOR: Evan F. Cihlar

Introduction and Background

The nature of modern warfare has changed, with a new "mix and match" multidimensional approach from aggressor states and their proxies. In the military sphere, this means attacks in one domain can lead to retaliation in another - military strikes following cyberattacks, for example. But, of more note, targeted or indiscriminate cyberattacks on civilian infrastructure and the commercial sector have become a softer and easier to reach target than locked down military or intelligence platforms. All of which is proving a challenge to traditional definitions of warfare. The blurred lines between the military and civilian domains and the ease by which cyberattacks can be launched on targets thousands of miles from home have become a game-changer. Military dominance is undermined if the home-front is woefully vulnerable to a catastrophic attack. While we read about long-range missiles being launched in countries, the fact is that a takedown of a country's energy grid of transportation network or health service is a far greater risk. That risk doesn't need any scientific developments and rogue supply chains - it exists today.

These new developments, all taking place under the broader umbrella of hybrid warfare (which also includes propaganda, spheres of influence, media manipulation and population interference) require new definitions, clarity, and ultimately, rule of law. The difficulty in direct nation-state attribution and the obfuscation of state-sponsorship of hacking groups is a serious issue for the practicalities of holding actors to account and ensuring that retaliation is directed at the right place.

Recent Attacks

In May 2019, Israel bombed and destroyed a building in Gaza, Palestine, as it was being used by a Hammas-backed hacking group to target Israel. This was the first instance when a state retaliated to a cyber attack with a real attack. In another more recent incident from June, the US targeted Russia's electric power grids using crippling malware in retaliation to Moscow-sponsored cyberattacks on US infrastructure. States around the world have been retaliating to new and persistent cyberattacks sponsored by their arch-rivals. According to a Thomson Reuters Labs blog, published in January 2019, countries facing the highest number of attacks include the US (65), UK (34), Germany (30), INdia (28), and South Korea (27). The blog claims that 22 countries are suspected of having sponsored cyber operations.

Many of these attacks have the support and financial backing of the state. A case in point is the Lazarus Group which incessantly targeted key industries including government bodies in the US< allegedly at the behest of the North Korean government in 2017-18, according to a report by McAfee Security. In some cases the cyberattacks were the handiwork of overzealous actors or terrorist groups and the country of origin may not have the resources to stop them. "There are cases where a government lacks the capacity to curtail groups operating from their territory. The challenge then is to credibly signal that to other countries on the receiving end, and to show that one is trying to improve the capacity to respond. That may also entail accepting help from the country that was attacked."

Cyber Warfare

Cyberspace, a domain created not by nature but by human beings, has emerged to provide tremendous benefits, but also presents new risks. Recently, cyber security has become a national policy issue. Driven predominantly by national security concerns, democracies have formulated national cyber strategies. For over two decades we have been hearing that "cyberwar is coming!" To the surprise of scholars familiar with the Realist theory of International Relations, the idea of Cyber War emerged alongside cyberspace conceptualisation and then realisation. History and philosophy show that scientific developments do not alter human nature enough to eradicate violent conflict. While the potential for using cyberspace in a conflict is obvious, the current prevailing properties of cyberspace make fundamental concepts of attack, defence, and ultimately war inadequate. However, even experienced defence and IT professionals all too often confuse acts of cyber crime and espionage with cyber attacks. Failing to conceptualise what cyber warfare is and, more importantly, what it is not, skews perception and results in faulty policymaking.

Risks and Materialisation

Technnologically indentical methods are used to gain unauthorised access to computer resources for most cyber operations, regardless of the intended purpose: crime, terrorism, industrial espoionage, military espionage, or warfare. Indeed, novel cyber attacks on critical national infrastructure are likely to severely disrupt social activities if successful. It has become theoretically possible to exploit the properties of today's cyberspace to attack strategic targets remotely. Furthermore, the attacker risks significantly less in cyberspace due to the widespread use of vulnerable commercial off-the-shelf technologies, the difficulty of distinguishing a glitch from malicious action, and the challenges of identifying the attackers. The discovery of "stuxnet" was the major driver for national cyber security. The threshold leading from cyber exploitation (espionage and criminal data theft) to physically destructive, politically-motivated cyber attacks was crossed in a spectacular manner. It remains the only known manifestation of a novel phenomenon: successful exploitation of cyberspace to target the control layer of a complex industrial process in order to achieve a destructive goal, all while avoiding military confrontation.

Cyberwar?

The unique properties of information and cyberspace make some of the familiar concepts inadequate. This paradoxical state of affairs testifies to the fundamental novelty of cyberspace that renders even millennia-old concepts of unsatisfactory. Stuxnet demonstrated just how sophisticated and precise cyber weapons could be, but to evaluate all cyber weapons' strategic effectiveness according to this specific case assumes too narrow a perspective. Website defacement, distributed denial-of-service (DDoS) massive cyber espionage - all are labelled “attacks;” some espionage operations are often upgraded to the “advanced persistent threat” monitor, and the whole scene is called “cyberwarfare.” War is a central experience of mankind that always had gruesome properties. “War is an act of force to compel the enemy to do our will;” it consists of several universal elements, famously formulated by Clausewitz. Centrally, war is a violent act, where the threat of force and violence is instrumental to achieving a political goal. Neither denial-of-service, web hacking, nor espionage are even potentially violent, even when Stuxnet is considered - no cyber incident has yet been violent nor caused loss of human life. Since none of the cyber events have yet met the requirements to constitute a war, the “cyberwar” metaphor should be relinquished, at least for the time being.

National Interventions in Cyberspace

The proponents of the internet as a self-organising global commons met national security strategies, along with the accompanying regulations and surveillance, with disapproval. Perhaps unsurprisingly, reliable evidence shows that the global commons ideal shunning state-led interventions is very remote from reality. Even liberal democracies employ domestic measures, such as content filtering and persistent surveillance for national policy ends, while confronting some opposition on legal, civil liberty and privacy grounds. The recent official national cyber strategies in developed democracies demonstrate a retreat from the long-term libertarian ideology that originally had shaped internet policy. The idea of the internet delimited into national sovereign networks was disdained in the West, with pundits labelling this scenario with the unambiguously negative term “balkanization.” However, the trend of national intervention in cyber is inevitable: once the crucial importance of cyberspace is acknowledged, nos tate can stay away from trying to assert cyber power. A constructive debate should focus on the decision-making process and the character of actions selected by national governments, instead of decrying the loss of an ideal.

Militarisation of Cyberspace: Meanings and Outcomes

Developed states have recognised the inadequacy of a laissez faire approach to cyber, but only after repeated cyber breaches had increased perceived insecurity did national cyber security policies became politically feasible. While analysing the national responses to cyber security challenges, light is shed on a pronounced trend towards the concentration of capacity in defence and intelligence circles. The accompanying over classification of the decision-making process regarding the means, goals, strategies, and activities severely stifles the public voice, increasing the conflict with the citizens' civil liberties. The severe suppression of public participation in the unfolding policy debate is anti-democratic. In practice, over-classification will be counter-productive. Cyber security is one of the most pronounced cases of multi-stakeholder governance where a subordination of all its facets to the national security establishment's perspective cannot provide a net-benefit outcome. Acknowledging this problem does not necessarily lead to the securitisation interpretation to which the critical security studies scholars adhere. For the "Copenhagen School," securitisation is an extreme version of politicisation that enables the use of extraordinary means in the name of security. But what if the strategic environment has undergone such a technology-driven change that methods previously considered extraordinary become vital? The vulnerabilities of cyberspace can be attributed to a protracted market failure of the IT industry. The business sector is justly recognised as essential for many facets of cyber security - but cannot do it alone. It also should not, just as we do not expect citizens or companies to defend from air-to-surface missiles by themselves, reasonably expect cyber security without a national security effort. The defence apparatus has an indispensable role to play in national cyber security and resilience, but it should be more closely controlled by democratic mechanisms.

Cyber Security: From a Technical-Military to a Democratic Approach

We cannot afford blissful ignorance regarding our changing environment.