Russia's Internet Research Agency and Cyberwarfare

https://www.e-ir.info/2023/12/05/russias-internet-research-agency-and-cyberwarfare/

CLARE STEVENS AND ANDREAS HAGGMAN, DEC 5 2023

This case study is an excerpt from McGlinchey, Stephen. 2022. *Foundations of International Relations* (London: Bloomsbury).

In November 2018, the US military blocked the internet access of a Russian organisation that had been seeking to sow discord amongst American voters during the midterm elections. According to US government officials, this operation against a company called the Internet Research Agency in St. Petersburg was a part of the first offensive cyber-campaign intended to thwart attempts to interfere with a US election. The operation was undertaken by a joint task force at the National Security Agency (NSA) and US Cyber Command, both of whom operate as part of the United States Department of Defense. The United States is not alone in establishing a military branch dedicated to ‘computer network operations’ – those deliberate actions that employ devices, computer programmes and techniques to create effects through cyberspace. Dozens of states around the world now have dedicated military units with this focus as seen on the Council on Foreign Relations’ Cyber Operations Tracker.

This case study seems to fit the bill for cyber warfare. However, when we look a bit more closely at the details and the political contexts of this operation, we can begin to see how the parameters of cyber warfare are still being worked out on the international stage. First, different states have different notions of what is ‘cyber’ about cyber warfare. This has important ramifications for the kinds of actions they can take, and the kinds of organisations involved. In this example, the United States military undertook this operation because the Internet Research Agency had been named as a key agent in a disinformation campaign that targeted American voters in the 2016 presidential election. Through falsified social media posts and targeted advertising, its goal was to ‘provoke and amplify political and social discord’ in the U.S., according to court documents issued after an investigation in 2016. Russia-backed content reached as many as 126 million Americans on Facebook during and after the 2016 presidential election.

The Internet Research Agency was not a military organisation but was still able to undertake a form of cyberwarfare. This is because Russia, led by Vladimir Putin (pictured), has a fundamentally different conception of the role of computer network operations. Russia does not generally use the term ‘cyber’ or ‘cyber warfare,’ except when referring to foreign approaches to the topic. Instead, like the Chinese, they conceptualise computer network operations within the broader rubric of information warfare (*informatsionnaya voyna*). The Internet Research Agency’s activities were thus viewed as an extension of longstanding Russian ideas about employing all state means, short of war, to achieve its national objectives. These actions are just one element of a wider spectrum of political subversion techniques, disinformation and psychological operations. In Russia, distinctions between peace and war are not as ingrained as they are in American strategic thinking. This conceptualisation of information warfare means that it is not only military or intelligence organisations that take part in Russia but a whole-of-state effort. Unlike the US approach, the Russian approach to offense is therefore not compartmentalised into military branches acting online.

Second, this case study highlights how cyber warfare is characterised by persistent low-level disruptions that are part of broader political actions, rather than a condition of a specified interstate conflict that takes place solely online. There may be many military units developing computer network operations capabilities globally, but this is not some devastating new form of warfare that a typical citizen can undertake. It takes a great deal of resources to undertake these kinds of operations. Furthermore, while state actors have reached broad consensus about what constitutes an ‘act of force’ in the context of cyberspace operations, in this example, both actors were careful to stay below this threshold under international law and the UN Charter. Instead, this new context is characterised by ‘persistent engagement’ – intense skirmishing that is part of a broader spectrum of actions rather than an isolated ‘weapon-like’ capability. As a case in point, the US government used criminal charges and indictments as well as sanctions in the case of the Internet Research Agency, demonstrating how computer network operations can also be used in conjunction with other tools of state power. Cyber incidents need not be responded to only with cyber-based retaliatory means.

This affair underlines the extent to which the parameters for cyber warfare are still being worked out for many states domestically as much as internationally. While Russia had been using a private company to undertake information operations, long held distinctions in US thinking between peacetime and wartime activities and military and non-military actors, together with the fact that the US was not formally in a state of war with Russia, meant that US Cyber Command would have had to get special authorisations . For example, a presidential order in 2017 gave Cyber Command greater latitude to undertake offensive operations below the level of armed conflict, without which they would have been legally constrained from targeting civilian organisations like Internet Research Agency. Furthermore, the Cyber Command operations appear relatively contained, especially in comparison with the increasingly sophisticated efforts by Russia to use disinformation to sow widespread dissent in Western countries. The American campaign undertaken in response to Russia’s information offensive is limited in large part to keep Moscow from escalating in response by conducting some reprisal that could trigger a larger disagreement between great powers.

Though the Internet Research Agency operations did not interfere with the election or voting processes themselves, which would have constituted an act of aggression under international laws of war, they did use connectivity to target individual voters’ relationships with those election processes. The operations also undermined confidence in the election processes. This also suggests the new types of challenges that authorities will increasingly face in protecting the individual in the cyber sphere from malign actors’ conduct. It also illustrates how cyber conflict is simultaneously a more prevalent and more mundane occurrence than the much more specialised practices of cyberwarfare. Yet, regardless of categorisation, the cyber realm is already becoming one where states are racing to establish superiority. In much the same way as air superiority and nuclear superiority emerged at key strategic points in the twentieth century, cyber superiority will increasingly be a buzzword of the future in political and military disputes.

About the author:

Clare Stevens is a Teaching Fellow in International Security with the Portsmouth Military Education team at the University of Portsmouth.

Andreas Haggman is Head of Cyber Advocacy at the United Kingdom’s Department for Digital, Culture, Media and Sport. He holds a PhD in Cyber Security from Royal Holloway, University of London.