Cyber Weapons as a Game Changer: A Critical Reflection

https://www.e-ir.info/2015/06/09/cyber-weapons-as-a-game-changer-a-critical-reflection/

ANDREAS HAGGMAN, JUN 9 2015

Cyber weapons are a game changer. At least, that is the case if we take at face value Marty Edwards' – head of the control systems security program for the US Department of Homeland Security – assertions regarding Stuxnet. It is certainly true that cyber weapons are a new weapon in the arsenals of militaries around the globe and that they represent innovative, some might say exciting, opportunities for exploiting the cyber dimension for warfare purposes. This piece will critically reflect on the characteristics of cyber weapons and the nature of war to explore the geopolitical dimensions of this topic.

Before delving into this it is first worth clarifying what is meant by cyber weapons. Perhaps the most useful definitions come from Thomas Rid and Peter McBurney, and Stefano Mele who all conclude that cyber weapons, in the form of weaponised code, are software which has the potential to cause damage. This damage may be physical, as in the case of Stuxnet, or it may be indirect and aimed at disrupting systems or influence human cognitive functions. Cyber weapons understood as weaponised code are distinguished from electronic warfare weapons; this distinction is useful as it invites new ways of thinking without being belaboured by archaic concepts which are not necessarily transferrable to the cyber domain.

Marty Edwards' assertions reflect popular conceptions about how cyber weapons are a game changer. These conceptions are popular insofar as they are widely held by policymakers and this has, in turn, trickled down to the general public, both through official rhetoric and popular media. In particular, these conceptions revolve around the specific characteristics of cyber weapons which set them apart from conventional kinetic weaponry. Often cited characteristics include stealth, range and speed. Though these are equally applicable to conventional weapons, it is argued that cyber weapons take each characteristic to a hitherto unknown level. The attribution problem, for example, enables cyber weapons to be deployed anonymously, or at the very least with plausible deniability. Conventional weapons like ballistic missiles are fired in a traceable trajectory allowing identification of the point of origin; cyber weapons have no easily discernible trajectory and are notoriously difficult to trace. Another key facet is the structure of modern computer networks, telecommunications and the Internet. Because connectivity is so ubiquitous, cyber weapons are able to reach any target across the globe and they are able to do this nearly instantaneously thanks to the speed provided by fibre optic cables. This extraordinary capacity for stealth, range and speed requires new ways of thinking about and planning for war. In essence, the equipment used to play the game has changed.

It can be argued, however, that such a view is too superficial to properly reflect the intricate nuances involved in war. Just because the equipment has changed this does not necessarily mean that the rules of the game, nor the players involved, have changed. Granted, the expertise required to manufacture and deploy cyber weapons is different from traditional weaponry, but the political structure within which they operate remains much the same. Monopoly on the legitimate use of violence is still the hallmark of a state, and it is the elites within states that make decisions on the commission and employment cyber weapons, as with other weapons. As a result (or potentially in defiance of!) this, the military adopts new technology with some great frequency – indeed, the military are often primary drivers of technology development. Throughout history, equipment like the stirrup, musket and tank have influenced *how* war is fought, but none of them have fundamentally changed the *reason* or *purpose* for war. Cyber weapons, following this

trend, are merely the next addition to the military arsenal; they do not obviate the enduring Clausewitzian nature of war. John Keegan has argued that the only weapons to do so are nuclear weapons, but it seems a step too far to equate cyber and nuclear given their disparate capacities for destruction.

Despite not being a fundamental game changer, cyber weapons nevertheless skew some basic assumptions about warfare. Specifically, because of their immateriality and (pseudo)anonymity, cyber weapons do not fit neatly into traditional calculations in war. Planning in geopolitics and international relations is underpinned by intelligence about other actors. This intelligence helps shape assessments of military capabilities and political intentions. With cyber weapons, such intelligence is very difficult to collect. In capability and intention calculations, cyber weapons therefore form an unspecified variable, which can significantly alter the outcome of the calculation. This can be applied to something like game theory, where traditionally the players have visibility of all options and outcomes and make decisions based on this. With cyber weapons thrown into the mix, visibility becomes shrouded and decision making becomes more uncertain.

In this sense, cyber weapons are game changing because they can influence the rationality of those who make political decisions. Incomplete situational awareness is unsettling and can foster doubt and fear, which in turn leads to irrationality. If those at the top are unsettled by cyber weapons, this disposition is likely to trickle down to the general public and affect societal attitudes towards cyber weapons. This phenomenon seems woefully unexplored in the current literature landscape, and deserves to be further elucidated and analysed.

The purpose of this piece has been to deconstruct and re-evaluate claims about the game changing properties of cyber weapons. It is important to be critical of such claims, as they are often based on misunderstandings of cyber weapons' capabilities. Despite not changing the enduring nature of war, cyber weapons are a new technology currently acting as a bit of a joker in the pack which potentially creates uncertainty in the geopolitical environment. Stealth, range and speed are attractive characteristics of cyber weapons, yet concentrating solely on the material effects ignores much of what war is really about. It is important to consider the whole spectrum of societal relations, both inter- and intra-national, when assessing the impact of new technologies such as cyber weapons.

About the author:

Andreas Haggman is a Doctoral Candidate in the Centre for Doctoral Training in Cyber Security at Royal Holloway University of London, where he is writing his PhD thesis on wargaming cyber-attacks.