The Potential Impact of Cyber Capabilities Upon Future Strategy

by Alessia Maira

ITSS Verona Magazine, Vol. 1, n. 2

Fall/Winter 2022

The Potential Impact of Cyber Capabilities Upon Future Strategy

Alessia Maira

To cite this article: Alessia Maira, *The Potential Impact of Cyber Capabilities Upon Future Strategy*, ITSS Verona Magazine, Vol. 1, no. 2, Fall/Winter 2022.

Keywords: Strategy, Cybersecurity, Warfare, Technology, Cyber-capabilities

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: December 30th, 2022

Abstract: The discussion around the potential impact that cyber capabilities could have on future strategy is ongoing. In particular, different opinions between scholars and experts of the field revolve around whether they might have a possible role in expanding the scope of conflicts and changing the perception of wars from a physical approach to a multidimensional one, or if they will remain an important but "peripheral" new asset, to be used in conjunction with traditional force as a rather subversive tool. This essay argues that while cyber capabilities have today become one of the key strategic assets of a state, their intrinsic nature makes it unlikely that they will gain primacy status over strategy for physical war making and cause a paradigm shift. As it was the case with the onset of nuclear weapons, cyber capabilities have a revolutionising potential and will continue to be extremely relevant in the years to come, but not by changing the current status quo. Rather, their influence will be visible from a multidimensionally wider strategic approach, for example, in order to achieve increased precision in air, sea and land operations, and under the form of subversive tactics that are part of a wider military and political strategy. The conclusion of this article is that they will influence strategy making as additional tools rather than cause a paradigm shift in how wars are fought and perceived.

Strategy and the cyberspace

Having come into existence only in the second half of the 20th century, cyberspace has changed the world forever and allowed humans to become instantly connected over large distances. While cyber capabilities are a relatively new asset among the many tools that are already available to states, they are continuing to revolutionise the world throughout the 21st century and will likely continue to do so for many years. As the use of cyber-related machines and applications has progressively gained momentum over the past few decades, they have also gained fame in popular culture and mass-media: a wide number of Hollywood movies have harnessed the concept of machines and computers taking over humanity and the world.

As opposed to the status quo revolution of 1945 that was the consequence of the use of nuclear weapons of mass destruction against Japan, which led to the primacy of deterrence over war, or, as the famous first-wave nuclear strategist Bernard Brodie put it, the goal went from winning a war, to avoiding a nuclear one at all costs,[1] there has been no such development in the use of (offensive) cyber capabilities. In fact, despite the growing strategic importance of the realm of cyber space in the past decades, most aspects that are related with cyber capabilities still remain widely debated and unregulated both at the academic, governmental, and international level. For example, a RAND publication of 1993 claimed that cyberwar was coming, and that the future of war would "be shaped in part by how these technological advances are assessed and adopted".[2] On the other hand, some experts of the field were (and still are) reluctant to define the cyber realm as a potential influence for changing the status quo as we know it today: in a study published in 2013 by Thomas Rid (about 20 years after the abovementioned RAND publication), it was argued that cyber war was not going to take place.[3]

---

[1] Bernard Brodie, *The Absolute Weapon*, New York: Harcourt Brace, 1946: 76.
[2] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *RAND Corporation Reprints*, (1993): pp. 23-60, https://www.rand.org/pubs/reprints/RP223.html, 25.
[3] Thomas Rid, "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): pp. 5-32, https://doi.org/10.1080/01402390.2011.608939, 6.

At the governmental level, the cyberspace was only included in the policymaking discussion in recent years, for example, no mention of the cyber domain is found in the US National Security Strategy document of 2002, and it is only briefly mentioned in the NSS of 2006 among the "disruptive challenges from state and non-state actors".[4] A swift change can be seen in the NSS of 2010 and then 2015, where cybersecurity and cyberthreats are mentioned as being a highly relevant aspect of security.[5] Furthermore, NATO recognised the cyberspace as one of its operational domains only as recently as 2016,[6] and at the international level, several discussions have taken place, but because of the intrinsic nature of offensive cyber capabilities, deterrence, regulations, and monitoring are difficult to implement, especially at a multilateral level.[7] This lack of international regulation is one of the issues that renders cyberspace strategy difficult to address in the international arena.

The "new" dimension of the cyberspace

Despite not having had the necessary influence to cause a shift in the status quo, the advent of cyberspace was able to change many other things related to strategy: for example, access to war. It is undeniable that throughout human history, technological developments have always promoted innovation and changed the approach to the latter and the means and strategies to how wars were fought.[8] In particular, warfighting in the cyberspace is clearly distinguished by a discontinuation from the classical approach to war, or what Clausewitz defined as "an act of violence",[9] instead, in the digital domain there is no direct violence. Rather, cyber-attacks have the intent to disrupt, cause economic loss, and inconvenience the enemy by targeting vital infrastructure, like it was the case

---

[4] The White House, "The National Security Strategy of the United States of America", 2006, https://georgewbush-whitehouse.archives.gov/nsc/nss/2006/, 44.
[5] The White House, "The National Security Strategy of the United States of America", 2015, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.
[6] NATO, "Cyber Defence", 2022, https://www.nato.int/cps/en/natohq/topics_78170.html.
[7] Mark Raymond, "Social Practices of Rule-Making for International Law in the Cyber Domain." *Journal of Global Security Studies,* no. 2 (2020): pp. 1-24, https://doi.org/10.1093/jogss/ogz065, 1.
[8] Martin Van Creveld. Technology and War: From 2000 B.C. To the Present. The Free Press, A Division of Macmillan Inc., 1991: 312.
[9] Brodie Bernard and Rosalie West, *On War*, Edited by Michael Howard and Peter Paret, Princeton University press,1984.

with Ukraine in 2015[10] or Estonia in 2022.[11] As a consequence of this, the cyberspace has allowed to expand the access to warfighting and disruptive operations: smaller and weaker states, as well as non-state actors (state-funded or not), have gained access to the international arena and are now able to interact with more powerful entities in a new dimension, without the need to harness physical force. In fact, the main characteristic of the cyberspace, which is also known as "the fifth domain of war"[12] – the others being land, sea, air, and space – is exactly what separates it from the other four: that it is not tangible or physical and exists only as a virtual operational domain.

Revolutionising, but only as a "new asset" among many

By looking at the available literature it is immediately obvious how opinions on cyberspace have varied through the years from cyber capabilities being the future of war making, to them having no real influence on it and being only an addition to the vast arsenal of strategic tactics that can be harnessed among other tools, as argued by Colin Gray.[13] In support of the position that argues the latter, the arguments surrounding the impact of cyber capabilities used for strategy making are the most convincing. Therefore, acknowledging the technological advancements that were permitted by cyber capabilities, but also recognizing their limits, is key in discussing why they have not had the same degree of influence on strategy (at least as of today) as nuclear weapons.

Anonymity as a grey cloud surrounding cyber capabilities

Another aspect that increases difficulties in implementing a strategic approach to cyberspace is anonymity and the grey cloud surrounding attribution. While on one hand anonymity in cyber-attacks presents a strategic advantage, misattribution on the other hand, is one of the risk-amplification issues that cyber capabilities carry. The anonymous and digital nature of cyber operations makes it very hard to attribute the origin of a specific action to a subject and,

---

[10] CFR, "Compromise of a power grid in eastern Ukraine", 2015, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.
[11] Andrius Sytas, "Estonia says it repelled major cyber-attack after removing Soviet monuments", 2022, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/..
[12] The Economist, "War in the Fifth Domain", 2010, https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.
[13] Colin S. Gray, "Making Strategic Sense of Cyber Power: Why the Sky is not Falling," www.babel.hatitrust.org, 2013: pp. 1-88, https://babel.hathitrust.org/cgi/pt?id=mdp.39015093428343&view=1up&seq=13&skin=2021, 13.

consequently, makes it easy to deny such responsibility. As a consequence of this, attribution in the cyberspace becomes a "slippery concept"[14] – as opposed to physical acts of force in traditional war making, in which (keeping in consideration the occurrence of undercover and false flag operations) attribution is usually easier.

Anonymity in operations is nothing new: it bears the same meaning and intent as physical undercover operations – which have existed throughout all human history. Classical strategists such as Sun Tzu argued that victory with the minimum effort (and bloodshed) was a peak achievement.[15] This is similar to the aim of cyber operations: achieving an end goal without the need to fight a physical battle, but rather from cyber capabilities. However, cyber operations might provide strategic value at the initial stage of the operation, but results in the long run are difficult to obtain, predict, and maintain.[16]

On the other hand, it can be argued that the grey cloud that surrounds attribution issues and anonymity in cyber operation poses a strategic advantage for actors that are physically weaker or smaller than their adversary or target. An increased usage of this approach by malicious states who wish to outsource to a non-governmental entity or group in order to avoid accusations might also be possible, as well as weaker or smaller states that might not have a military advantage over a stronger or larger state who could still be able to interfere with the latter, as in a "David vs Goliath" scenario. However, as it is often difficult to attribute responsibility correctly, this might lead to confusion in the international arena as well as misplaced accusations and escalating tensions, and these aspects also have a relevant detrimental influence on the overall strategic value of these kind of operations. Remembering the latter is key in understanding the potential risk amplification value that difficulties in attribution and anonymity might cause, and their consequences on strategy in cyberspace.

---

[14] Michael Poznansky, "Revisiting Plausible Deniability." *Journal of Strategic Studies*, no. 2 (2020): pp. 1-23, https://doi.org/10.1080/01402390.2020.1734570, 1.
[15] Sun Tzu, The Art of War. Dover Publications, 2002.
[16] Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security,* no. 2 (2021): pp. 51-90, https://doi.org/10.1162/isec_a_00418, 51.

Not only offensive: the defensive aspect of cyber capabilities

Technological innovations throughout history have always led to innovative strategic advancements in war making.[17] The use of offensive cyber capabilities in strategy making for war has allowed to achieve greater precision in operations and the ability to use unmanned vehicles in dangerous areas; and new technologies such as unmanned drones can be seen as yet an extension of airpower, eliminating the risk of human loss during operations (both of innocent civilians and operatives), as well as providing relevant data "about terrain, environmental, and tactical conditions that can be communicated to troops and their command instantaneously".[18]

Apart from the offensive advantages that technological developments can offer, the defensive aspect of cyber capabilities must be also kept in consideration as a primary tool of strategy making in the fifth domain. In fact, with the advent of cyberspace, vital infrastructures became vulnerable not only to traditional attacks – those that use physical kinetic force – but also to non-physical cyber attacks, which can be used as a politico-economic weapon in the same manner as traditional attacks. Without the need to cross any geographical border, attacks of this kind make it possible to engage with actors who are distant by targeting their general infrastructure such as power grids, nuclear stations, banks databases, and data in general. Examples like the Stuxnet affair of 2015, which was key in increasing the attention to cybersecurity,[19] prove that the most relevant potential of cyber capabilities used by a state is the ability to engage with the cyber realm without the need to cross any physical border: as the web has no tangible geographical borders, state or non-state cyber agents can undertake intelligence gathering or disruptive operations that in the past would have otherwise required the use of spies or undercover agents.[20]

---

[17] Christopher Coker, Future War. Polity Press, 2015: 56-68.
[18] The White House, "Maintaining Military Advantage Through Science and Technology Investment.", 1995, https://clintonwhitehouse4.archives.gov/WH/EOP/OSTP/nssts/html/chapt2.html#:~:text=Advances%20in%20information%20technologies%20contribute,troops%20and%20their%20command%20instantaneously.
[19] Alexandra Van Dine, "After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities", *Center for Strategic and International Studies*, (2017).
[20] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): pp. 5-32, https://doi.org/10.1080/01402390.2011.608939, 17-20.

The possible primacy of defensive over offensive abilities

Although offensive cyber capabilities are the most heard and discussed online and in the news, and there is a perceived higher "threat" of offensive cyberspace operations in mass media and public opinion, a state must be ready to defend itself as much as it is capable of launching a cyber-based attack or operation. In fact, it has been discussed how it is much more costly to defend oneself against cyber-attacks than it is to sponsor one.[21] This shows that there is a possible primacy of defensive over offensive cyber capabilities. In fact, as regulating the cyber space internationally and through multilateral agreements has proved to be difficult if not impossible to be achieved (at least as of current times), more and more states have begun to give greater importance to the defensive aspect of cyber capabilities and are conceptualising a strategic approach to their defensive abilities. In relation to the relevance of the defensive aspect in the cyber realm, it is also relevant to mention that rapid evolution and expansion of this dimension have led to a different level of readiness and experience on the topic among states. Therefore, it is arguable that their relevance for future strategy discourse and policymaking will keep gaining momentum in the years to come, and also that giving primacy to defensive (rather than offensive) cyber capabilities might be the best way forward for strategy making in the cyber era.

Conclusion

In conclusion, while there are strategic advantages to cyber capabilities like anonymity, increased precision in air, sea and land operations, greater access for state and non-state actors, and lower offensive costs, the intrinsic nature of these kinds of attacks are negatively affecting their potential to gain traction and cause a shift in the status quo of war fighting, as much as they are posing challenges to the development of strategy related to the cyberspace. However, despite the challenges that they present, they remain relevant for strategy making and also for having revolutionised the approach to the latter by creating a new dimension in which wars and offensives

[21] See note above, 27-28.

can be launched, and, at the same time, for expanding the key strategic and defensive aspects that must be addressed by states for accurate strategy-making.

At best, the increase in cyber-based operations might remain solely another tool that a state can harness, for example in the form of subversive tactics, used as part of a greater offensive and political strategy, while at worst, they might become the new way of launching a "war-opening attack", with the potential to escalate tensions and eventually lead to the traditional physical war fighting and application of violent physical force. In both instances, states must have a cyber strategy in place and be prepared to defend themselves and their vital infrastructure.

Bibliography

Books

Bernard, Brodie, and Rosalie West. On War. Edited by Michael Howard and Peter Paret. Princeton University Press, 1984.

Brodie, Bernard. The Absolute Weapon. New York: Harcourt Brace, 1946.

Coker, Christopher. Future War. Polity Press, 2015.

Tzu, Sun. The Art of War. Dover Publications, 2002.

Van Creveld, Martin. Technology and War: From 2000 B.C. To the Present. The Free Press, A Division of Macmillan Inc., 1991.

Journal articles

Maschmeyer, Lennart. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security*, vol. 46 no. 2, (2021): 51-90. https://doi.org/10.1162/isec_a_00418

Poznansky, Michael. "Revisiting Plausible Deniability." *Journal of Strategic Studies*, vol. 20 no. 2, (2020): 1-23. https://doi.org/10.1080/01402390.2020.1734570

Raymond, Mark. "Social Practices of Rule-Making for International Law in the Cyber Domain." *Journal of Global Security Studies*, vol. 6 no. 2, (2020): 1-24 (ogz065). https://doi.org/10.1093/jogss/ogz065

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies*, vol. 35 no. 1, (2012): 5-32. https://doi.org/10.1080/01402390.2011.608939

Conference papers

Van Dine, Alexandra. After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities. Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series, Center for Strategic and International Studies (CSIS), (2017).

Online sources

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *RAND Corporation Reprints, 1993.* https://www.rand.org/pubs/reprints/RP223.html

CFR, “Compromise of a power grid in eastern Ukraine.” CFR, December 2015. https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

Gray, Colin S. "Making strategic sense of cyber power : why the sky is not falling.", 2013. www.babel.hatitrust.org, https://babel.hathitrust.org/cgi/pt?id=mdp.39015093428343&view=1up&seq=13&skin=2021

NATO. *Cyber defence,* 2022. Accessed online on June 24th 2022. https://www.nato.int/cps/en/natohq/topics_78170.html

Sytas, Andrius. "Estonia says it repelled major cyber attack after removing Soviet monuments." Reuters, August 18th, 2022. https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/

The Economist. "War in the fifth domain.", July 1st, 2010. Accessed online on June 23rd 2022. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

The White House. "The National Security Strategy of the United States of America." The White House, President George W. Bush, 2006. Accessed online on June 21st 2022. https://georgewbush-whitehouse.archives.gov/nsc/nss/2006/

The White House. "The National Security Strategy of the United States of America." The White House, President Barack Obama, 2015. Accessed online on June 21st 2022. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

The White House. "Maintaning Military Advantage Through Science and Technology Investment.", 1995. Accessed online on June 19th 2022. https://clintonwhitehouse4.archives.gov/WH/EOP/OSTP/nssts/html/chapt2.html#:~:text=Advances%20in%20information%20technologies%20contribute,troops%20and%20their%20command%20instantaneously