This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

# Review - The Hacker and the State

https://www.e-ir.info/2020/06/11/review-the-hacker-and-the-state/

ANTONIO CALCARA, JUN 11 2020

***The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics***
**By Ben Buchanan**
**Harvard University Press, 2020**

If you believe that cyber attacks are now critical to understand today's International Relations (IR), stop doing everything you are doing and start reading Ben Buchanan's new book *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. The book provides an innovative theoretical perspective to understand cyber attacks, which will certainly be of interest to every IR pundit and student. While Buchanan's previous contribution focused on how to apply IR's security dilemma to the emerging reality of cyber conflicts, the present book assesses the implications of cyber attacks for the so-called concept of signalling. The concept, introduced and developed (among others) by the Nobel prize for economics Thomas Schelling, describes how certain strategic tools (military exercises, conventional military capabilities, nuclear weapons and so on) are mainly used by states to communicate to each other and, ultimately, to try to change or coerce an opponent's behaviour in international politics. To make a striking example, NATO's frequent exercises on Europe's eastern flank may be interpreted as signals to show the readiness of the alliance vis-à-vis its Russia neighbour. Nuclear weapons tests are perhaps signals in their purest form.

In contrast to these examples, cyber attacks are a weapon that can achieve a wide range of objectives but fail at signalling. Cyber attacks are indeed ill suited to attempts to change or coerce an opponent's behaviour and are most effective when conducted in secret. Exposure to the public domain can be dangerous for the hackers (and for the states that support/finance them), but would also make them deeply ineffective at signalling and, ultimately, in changing or coercing the opponent's strategies in international politics. The nation that hacks best and without being exposed will triumph. Throughout the book, Buchanan makes clear how we need to pay attention to the distinctiveness of cyber attacks and the strategic logics behind them.

In order to test this argument, Buchanan takes us on a journey into the "fascinating" (and very often frightening) world of hackers and the states that support and finance them. The author is a profound expert of this world and knows the most complex technical ramifications of cyber attacks, now a low grade yet persistent part of geopolitical competition. The empirical part of the book is therefore structured into three sections, which re-group different cyber attack operations according to their goal: espionage, sabotage, destabilization.

In the first section, Buchanan accurately describes the complex espionage system put in place by the US' National Security Agency (NSA) and by the Five Eyes alliance (Australia, Canada, New Zealand, UK, US). The author is particularly convincing when outlining the "home field advantage" enjoyed by the US, because of its critical position along the key digital hubs, infrastructures and cables that connect the globe. US telecommunications providers such as AT&T and Verizon have customers all over the world and American corporations are also the pivot on which internal modern digital ecosystems are based. Just think about Google, Facebook and Amazon. The alliance between the US and its digital businesses, for instance the PRISM agreement between Washington and Microsoft (and then extended to Google, Facebook, Apple and Yahoo), has allowed the US to be able to collect an impressive mass of data and information that extends across the globe. In contrast, China cannot enjoy this home advantage

and – notwithstanding its aggressive espionage operations (especially towards US industrial and military production) – it has been unable, at least so far, to build a network of intelligence systems comparable with that of the US and its allies.

The second part of the book focuses on sabotage, presenting four important cyber attack operations. The first two cases refer to the famous targeted sabotage operation Stutnex, targeting Iranian nuclear plants (reportedly designed by the US and Israel) and to the Iranian hackers' attack against the Saudi oil company Aramco. Buchanan then describes why the Stutnex operation can be considered the more effective of the two. While the Stutnex operation was indeed conducted in secret, in the second the Iranians wanted to signal their presence. Despite the significant economic damage they caused, Iranian hackers have not been able, as the signalling argument would posit, to somehow change or coerce Saudi Arabia's behaviour vis-*à*-vis Teheran. The third and fourth cases refer to the massive hacking operation of North Korea against Sony (due to the release of controversial film "The Interview") and the two blackouts caused by Russian hackers against Ukraine. These two examples show, as Buchanan clarifies, how "cyber operations were only getting more powerful and hackers were only getting more aggressive" (p.207). However, according to the author, both operations were ineffective in changing or in some way coercing the US or the Ukraine's behaviours against Pyongyang or Moscow.

The third part, related to the destabilization caused by cyber attacks, starts from an event that has had wide resonance in international public debate: Russian interference in the 2016 US election. Buchanan masterfully describes, through an impressive range of primary and secondary sources, all the details behind the Russian hackers' operation against the Democratic Party's digital infrastructures (starting from the mail of its most relevant representatives) and the disinformation campaign that they fuelled through social media. This section also offers entertaining anecdotes, such as when Buchanan describes the North Korean hackers' fraud against the Bank of Bangladesh, partially foiled by the fact that the hackers made a typo that allowed the authorities to save up to $850 million. This typo is, probably rightly, defined by the author as "one of the most expensive in history" (p. 274).

Buchanan is very convincing in showing the growing aggressiveness of modern cyber operations. If there is a clear pattern, the author writes in the conclusion, it is that "the harm that hackers can do is expanding faster than the deterrence of defences against them" (p.313). The tone of the conclusions is in fact slightly pessimistic, especially when he discusses the limits of what to do diplomatically against cyber attacks. More specifically, "naming and shaming" against Russian, Iranian or North Korean hackers, as well as Chinese industrial espionage have not been effective measures to change these states' conduct. Moreover, the fact that Western states' espionage systems have been also exposed (see the first part of the book on the NSA) certainly does not help the international legitimacy of cybersecurity efforts by these actors. These considerations are also at the centre of the current geopolitical discussion, considering the US' strong pressure towards its allies – with mixed results – to ban the Chinese company Huawei from developing 5G infrastructures for cybersecurity reasons. Some states may be realizing that cyber attacks used for geopolitical goals will remain in any case a persistent feature of international politics.

However, the author is also able to put things into perspective highlighting the complexity of the current (geo)political situation, of which cyber attacks are just one (though not a marginal) component. As regards the much-debated Russian interference in the 2016 US election, he writes that "the Russian wedge widened underlying divisions in the United States on hot-button issues. It did not have to create racial tensions and ideological differences; they were already there waiting to be exploited" (p. 238). I have already written for E-IR on how the growing mistrust in established authorities is indeed fertile ground for disinformation campaigns and fake news and, naturally, for cyber attacks.

The book is an incredibly informed examination of the cyber attacks that have taken place in recent decades. After a few chapters of the book, the reader may be stunned by the amount of information (and its level of complexity). More frequent steps back from the author would have allowed the reader to better process this amount of information and would have been beneficial for the overall readability of the book. From a more theoretical point of view, the author could have made a better effort to place his contribution within the recent literature on the subject. For instance, it is not clear how the author positions his theoretical contribution vis-à-vis important works by scholars such as Lucas Kello and Tim Maurer (among others) that are establishing more "traditional" links between the strategic logics of

cyber attacks and the IR scholarship. Moreover, a fruitful research avenue would have been to explicitly connect the home-field “espionage” advantage played by the US with the recent literature on weaponized interdependence. This would have been beneficial to link cyber attacks to a growing trend towards the “weaponization” of trade, industrial and technology policy. Despite this, the book is an incredibly informed examination of the cyber attacks that have taken place in recent decades. Overall, the book is a solid and much needed academic contribution to the IR cyber space literature. Cyber attacks are now an established reality. Buchanan’s contribution is a good starting point to make geopolitical sense of them.

---

### About the author:

Antonio Calcara is a post-doctoral researcher at LUISS University in Rome. He won the Egmont and the European Security and Defence College “Global Strategy Ph.D. Prize” in 2019 and is the author of European Defence Decision-Making: Dilemmas of Collaborative Arms Procurement.