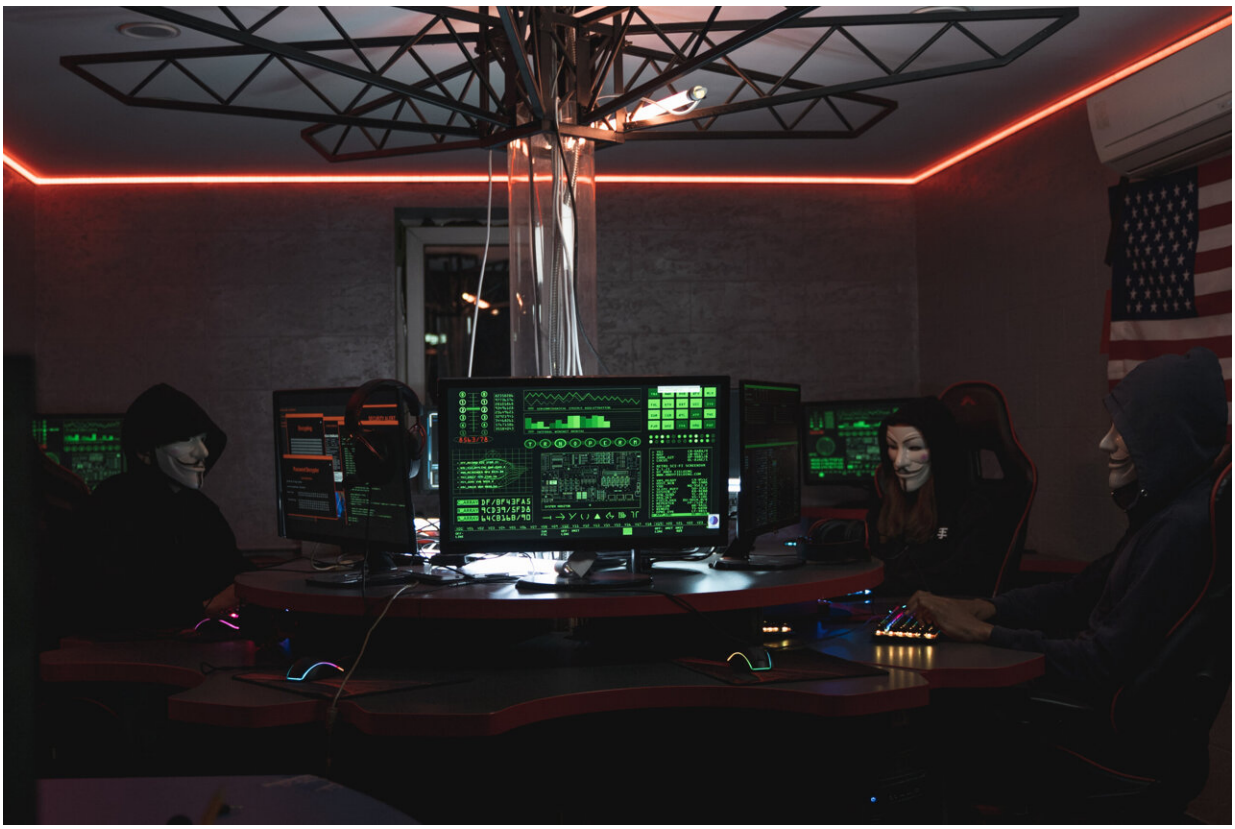
Trusting hackers with your security? You'd better be able to sort the whitehats from the blackhats

July 10 2015, by Mariarosaria Taddeo



Credit: Tima Miroshnichenko from Pexels

To think that men are so foolish that they take care to avoid what mischiefs may be done them by polecats or foxes, but are content, nay,

think it safety, to be devoured by lions.

English philosopher John Locke's words from 1689 describe the way in which fear for their own security may irrationally drive citizens to accept the absolute authority of the state. His words may bring to mind the NSA surveillance scandal, or more recently the devastating hack of cybersecurity firm Hacking Team.

The controversial "security" firm – parlance for hackers for hire – had its servers compromised, company files stolen and social media and email accounts hijacked. Some attribute the attack to activists aiming to expose the firm's dealings with authoritarian regimes – the 400Gb file the attackers posted online contains details that apparently support the concerns of Reporters Without Borders and the University of Toronto's CitizenLab.

Other believe the attack originates from a competing firm. In any case, what it demonstrates is that hackers today – as much as the well-funded government intelligence agencies – can affect national and international politics, to foster or to disregard human rights and ultimately to shape the development of democracy.

Striking the balance

Communication technology has become both a valuable asset needing protection and the means of attack. A balance must be struck between the rights of citizens – privacy, freedom of speech and information – and the requirements of the state to keep them safe and to secure itself against outside and inside threats.

The debate over the use of encryption is a case in point: on one hand encryption shields its users from intrusive surveillance, protecting their privacy. On the other, by thwarting the surveillance of law enforcement,

encryption limits the state's ability to protect its citizens. Striking a balance between individual rights and security is not a simple matter – Hobbes and Locke debated the problem centuries ago and it has been debated ever since. But the attack on Hacking Team reveals something more.

The new lords of the internet wild west

The term "hacker", aside from suggesting a high level of technical expertise, fails to take into account the wide range of aims and motivations moving these experts, for example hacktivism, crime, or terrorism. Hackers are not just tech-savvy experts – they are the new makers, capable of shaping debate and consequently the path societies take. Look at their role in the events of the Arab Spring, those fighting regulation of intellectual property and copyright, and groups like the Syrian Electronic Army (or Hacking Team) that support governments' intelligence activities.

More worryingly this hack, like the many others before it, reveals the unregulated grey area in which hackers operate. Hacking Team, based in Italy, has always denied accusations that it works with authoritarian governments, including those for which European Union member states are under arms embargos, such as Sudan. But will the details now revealed lead to any action against the firm? Were its actions illegal under national or international law? It's just not clear.

What is clear is the regulatory vacuum and lack of any effective restraints on the activities of hackers and cybersecurity firms, and the inability to distinguish legitimate from illegitimate uses of hacking expertise. Indeed, many working in the field cross from being "blackhat" (illegal) to "whitehat" (legal) operators. The distance between the two is often paper thin.

Bringing light to the shadows

Hackers prefer acting in the shadows, affording them anonymity and room for manoeuvre. Governments and intelligence services may favour a similar approach, allowing them to operate outside various constraints. But in the long run, information societies – especially democratic ones – cannot afford the risks of allowing this activity to remain in the shadows. As Locke pointed out, left to their own devices, the apparent saviour has the potential to become the next lion.

There have been attempts to regulate cybersecurity firms: the Wassenaar Arrangement, for example, defines rules controlling the export of surveillance software to specific countries. Very recently, the US Bureau of Industry and Security recently defined new rules based on the Wassenaar Arrangement. Although this showed a few significant drawbacks, the new rules are so broad that while forbidding collaboration with blacklisted counties they could restrict the legitimate use of tools used to improve computer security.

Such shortcomings are common when lawmakers attempt to regulate areas with which they are unfamiliar, overlooking their novelties and peculiarities. This has exacerbated the policy vacuum. The same can be seen in the application of the right to be forgotten in Europe, and the regulation of cyber-warfare.

The internet is the new realm with vital importance for all of us – and hackers are the masters of it, with the potential to bring about radical change, reshape the political status quo and redefine our understanding of political power. Until this is understood in the context of the current information revolution, any attempt to legislate and regulate the role of the hacker is doomed to failure.

Commons-Attribution/No derivatives).

Source: The Conversation