Book Review: The Internet in Everything: Freedom and Security in a World with No Off Switch by Laura DeNardis

In **The Internet in Everything: Freedom and Security in a World with No Off Switch**, **Laura DeNardis** *offers an exploration of the invisible, complex and concerning worldwide network of technologies often referred to as the Internet of Things, focusing particularly on the pressing issues of governance and jurisdiction.* **Courteney J. O'Connor** *highly recommends this well researched and impeccably written text to political scientists, security practitioners and scholars as well as the interested public.*

***The Internet in Everything: Freedom and Security in a World with No Off Switch*. Laura DeNardis. Yale University Press. 2020.**

One of the most pressing concerns in contemporary cybersecurity scholarship is how the 'Internet of Things' is affecting, and will affect, both individual security and privacy and the security of the state. As more and more devices connect to the internet and become integrated into every aspect of daily life, there is an ongoing battle between device efficacy and device security, between device utility and individual privacy, between security threat and threat mitigation.

Items as simple as Fitbit watches, for example, release enough data into the ether that entire military bases have been mapped based on soldier movements. Digital devices are woven into the fabric of everyday life in contemporary societies, and the internet has become so integrated that it is also becoming invisible: many people may not actually realise that their (many) smart devices are connected to the internet at all. This growing Internet of Things, this burgeoning network of digital and interconnected devices, is rapidly diminishing the line between physical and virtual, between connected and switched off, between logged in and logged out.

The Internet in Everything is an exploration of this invisible, complex and concerning worldwide network of technologies that we refer to as the Internet of Things, or the IoT. More specifically, author Laura DeNardis explores the consequences, proven and potential, of the degradation of and attacks on cyber-physical infrastructures. Governance and jurisdiction are particularly pressing concerns that are masterfully examined throughout the text.

> The Internet is no longer merely a communication system connecting people and information. It is a system connecting vehicles, wearable devices, home appliances, drones, medical equipment, currency, and every conceivable industry sector. Cyberspace now completely and often imperceptibly permeates offline spaces, blurring boundaries between virtual and physical worlds (3).

As an evaluation of the current state of the IoT, DeNardis produces here one of the starkest and clearest statements available to scholars and practitioners of security whose work has any relevance to cyberspace. The internet has truly become part of every aspect of not only individual lives, but also of the systems and structures that form the very foundation of modern society. We are, in fact, so reliant on networked technologies that as well as being extremely valuable to the wealth and security of most (if not all) states, cyberspace is also an issue of serious concern with respect to the security of systems that support the governance and functions of not just individual nations, but the entire international system.

Date originally posted: 2020-11-08

Permalink: https://blogs.lse.ac.uk/usappblog/2020/11/08/book-review-the-internet-in-everything-freedom-and-security-in-a-world-with-no-off-switch-by-laura-denardis/

Blog homepage: https://blogs.lse.ac.uk/usappblog/

This raises many questions about the method and efficacy of security measures given the multitude of threat vectors as well as the ways that security might change as society continues to advance and rely on networked technologies. This will have implications for the structure of the workforce, the types of technologies (and infrastructures) required and the jurisdiction over and governance of these same elements. As DeNardis asks early in the text, 'what does the Internet embedding into the physical world mean for consumer safety and national security?' (4). After all, cyber-enabled technologies are not only in devices around us; they are also now in devices that can be placed inside us. Any individual with a modern implanted cardiac device, for example, is an active part of the IoT. The body, just as much as the surrounding built environment, has become part of the digital object space. New technologies and new varieties of devices connecting to the internet, DeNardis rightly points out, are going to require a reassessment of and novel approaches toward internet governance and the cyber-physical infrastructure that underpins our increasingly networked societies (24). In other words, we now have an Internet of Everything.

Cyber-physical systems can safely be described as ubiquitous, particularly in societies that have embraced advanced technologies and platforms as part of daily life and efficient governance. The enormous variety of devices that form part of this global network includes everything from footballs to door locks, light bulbs to oxygen monitors, televisions to watches, traffic cameras to refrigerators, many of which are also connected to home assistants ('Alexa, turn off the lights') and/or controlled by a phone app. This means a continual stream of data between appliance and controller, usually transmitted (at least in part) over public internet and potentially unsecured networks (29-31).

All of these items, devices and systems represent new threat vectors, the true vulnerability of which may not be immediately apparent until an enterprising mind decides to take advantage. DeNardis uses as an example the case of hackers accessing and exploiting the network of a casino by first infiltrating the WiFi-connected fish tank (103). While an amusing anecdote, it is also an alarming and clear example of the vulnerabilities that are proliferating across public and private spaces.

Exploitation of cyber-physical infrastructures can even contribute to threats against political sovereignty, notable in the cases of disinformation and interference campaigns against the elections of modern democracies. Information warfare can be undertaken utilising data exfiltrated illegally (and usually covertly) from 'secure' systems – social engineering, already advanced in many ways, becomes much more highly targeted and tailored when data is available in significant quantity (106-107). This, of course, has many implications for the legitimacy of governance and authority, as well as the integrity of and public trust in democratic institutions such as elections.

Date originally posted: 2020-11-08

Permalink: https://blogs.lse.ac.uk/usappblog/2020/11/08/book-review-the-internet-in-everything-freedom-and-security-in-a-world-with-no-off-switch-by-laura-denardis/

Blog homepage: https://blogs.lse.ac.uk/usappblog/

That the physical infrastructures that support the global internet are within (and cross) sovereign borders is something that tends to be forgotten, due to the prevalence of claims about the decentralisation and border-agnostic nature of data and logical architecture (189). This requires, and has yet to receive, a global approach to infrastructure, policy and security to secure the future openness and freedom of cyber-physical technologies and networks. Because no one state (or more appropriately, the private corporations of one state) control the entirety of the infrastructure of cyberspace, a multilateral approach to the problems surrounding cyber vulnerabilities and the diffusion of insecure cyber-enabled technologies is a necessity going forward. DeNardis identifies the need not only to move from a content lens (concerning freedom of speech, disinformation, intellectual property) to an infrastructure lens (concerning platforms and systems) in discussions of cybersecurity, but also to recognise that cybersecurity is a growing human rights issue, and that greater clarity surrounding liability and jurisdiction in the cyber-physical space is needed – and quickly (215).

This is a very well researched and impeccably written text. While dense in terms of the information and discussion provided, particularly in the sections concerning the technical areas, *The Internet in Everything* remains easy to read and the lines of argument and discussion are clear and succinct. I do not hesitate to recommend this volume to political scientists, security practitioners and scholars as well as the interested public.

- *This article originally appeared at the LSE Review of Books.*
- *Image Credit: Photo by Franck on Unsplash.*

Please read our comments policy before commenting.

Note: This article gives the views of the authors, and not the position of USAPP– American Politics and Policy, nor of the London School of Economics.

Shortened URL for this post: **https://bit.ly/32iubtm**

About the reviewers

Courteney J. O'Connor – *The Australian National University*
Courteney J. O'Connor is a PhD candidate with the National Security College of The Australian National University. Her research considers the securitisation of cyberspace and the development of cyber counterintelligence policy and practice.