ISS/NASA

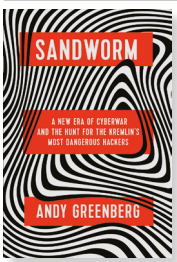
Ukraine's electricity grid has been hit by several cyberattacks (photo from 2019).

The growing rumblings of cyberwar

Andy Greenberg is trenchant on the mounting capacity of malware to wreak havoc. **By Brian Nussbaum**

In 2017, a piece of malicious software called NotPetya launched the first global data-destruction pandemic. It was probably the most expensive cyberattack in history. The culprit was Sandworm, an aggressive, malicious hacking group, which many analysts linked with Russian military intelligence. Technology journalist Andy Greenberg's eponymous book tracks the group's attacks, and the people and companies that chase them across computer networks worldwide. It also spells out the implications of the hackers' destructive agenda for all of us.

Greenberg recounts the details of the group's record since at least 2014. He draws on his reportage for *Wired* on the 2015 and 2016 attacks on the Ukrainian electrical grid, which led to serious blackouts and left hundreds of thousands of Ukrainians without power. In addition to NotPetya, he examines other attacks conducted by, or affiliated with, Sandworm. These range from strikes against election infrastructure in several countries, including the United States, to the 2018 winter Olympic Games in South Korea, and international treaty organizations such as the Organisation for the Prohibition of Chemical Weapons in The Hague, the Netherlands.



Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers
Andy Greenberg, Doubleday (2019)

Sandworm is particularly disturbing for several reasons. Its malware is sophisticated and capable. Its targeting illustrates troubling recent dynamics in cybersecurity – including escalating disruption, the ability to destroy data or create physical damage and the targeting of crucial civilian infrastructure.

By contrast, most cyberattacks have focused on the theft or exposure of data, exploiting this for financial gain or strategic advantage. We know such data breaches all too well from criminal and spying activity, such as credit-card data being stolen from large retailers, or the mammoth 2015 breach at the US Office of Personnel Management in Washington DC. Whether what was taken was financial data or strategically important secrets for espionage, the impacts of cyberintrusions tended not to create immediate concerns about the safety of individuals or the stability of global economic or political structures. Many commentators thus downplayed the rhetoric that surrounded them.

For many years, however, military and intelligence officials and other commentators in the United States often spoke of the possibility of a "cyber Pearl Harbor" or "cyber 9/11". Some warned consistently of "cyberwar", although many cybersecurity experts bristled at the suggestion that computer crime and espionage efforts warranted the term. Political scientist Thomas Rid aired that scepticism in his 2013 book *Cyber War Will Not Take Place*.

NotPetya was a turning point. It deployed what looked to be ransomware, using a 'back door' in a Ukrainian tax-preparation software package. Ransomware encrypts a computer's files and offers to sell users a decryption key for a ransom, often paid in cryptocurrency such as Bitcoin. Greenberg shows how, while seemingly targeting Ukraine, the malware spread rapidly around the world. And although it seemed to be conventional ransomware, it did not offer a real way to decrypt files.

Greenberg details how NotPetya led to many firms incurring costs of hundreds of millions of dollars. They included pharmaceuticals giant Merck, shipping conglomerate Maersk, FedEx subsidiary TNT Express, French construction company Saint-Gobain and US food producer Mondelēz. Tom Bossert, former homeland-security adviser to US President Donald Trump, confirmed to Greenberg that global losses were estimated to top US$10 billion. Even Rid told Greenberg that if "anything comes close to cyber 9/11", it is NotPetya.

In the past decade or so, physical systems

– from stop lights to electrical grids to pacemakers – have become increasingly connected to, and controlled by, computers. Greenberg uses Sandworm to show how threats have grown from assaults on systems that collect and process information, to assaults on *systems* that control physical devices and processes. From insulin pumps, to dams, to entire transport networks, the increasing reliance on computers to run the things around us has made the potential impact of cyberstrikes much more grave. Malicious computer code might prompt a crucial industrial device to overheat and cause a fire, explosion or other damage – as happened to a German steel mill, according to a 2014 report by Germany's Federal Office of Information Security.

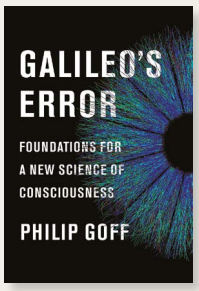
Sandworm was not the first group to damage physical infrastructure with malware, however. That was the team behind Stuxnet, which destroyed centrifuges at the nuclear power plant in Natanz, Iran, disrupting uranium enrichment. David Sanger at *The New York Times* attributed Stuxnet to a mix of US and Israeli intelligence and security agencies. But Sandworm, by hitting the Ukrainian electrical grid, has drastically ramped up concerns about protecting civilian targets. Greenberg documents how the group has created malware designed to manipulate and harm control systems across borders, software and hardware platforms, and industry sectors.

In an era of fake news and disinformation, determining whether hackers are who or what they seem can seem a daunting task. Yet anonymity in cyberspace is often overstated. Despite the challenges in identifying culprits who have the capacity to hide and to leave false trails, many governments and, increasingly, private organizations, are capable of doing it. Greenberg shows how researchers, firms and agencies, from big software companies to private-sector actors, are responding to Sandworm and other cyberthreats. The result? Hackers have been subjected to exposure and publicity; security firms have blocked their tools; and their members and leaders have been indicted.

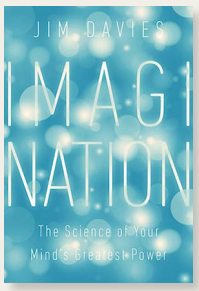
Sandworm offers an important front-line view of the changing cyberthreats that are shaping our world, their creators and the professionals who try to protect us.

Brian Nussbaum is an assistant professor at the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University at Albany, part of the State University of New York. A former intelligence analyst, he is also a cybersecurity fellow at the New America think tank in Washington DC, and an affiliate scholar with the Center for Internet and Society at Stanford Law School in California.
e-mail: bnussbaum@albany.edu

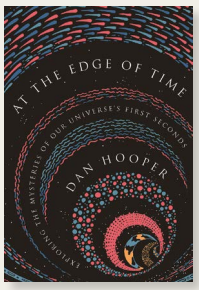
Books in brief



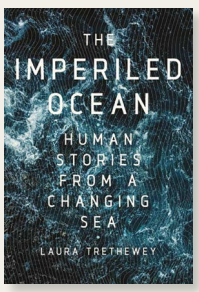
Galileo's Error
Philip Goff Pantheon (2019)
In this well-argued, but provocative, study, philosopher Philip Goff asserts that "nothing is harder to incorporate into our scientific picture of the world" than consciousness. Goff harks back to 1623, when physicist Galileo Galilei adopted a dualist position: consciousness exists completely outside the physical realm. Today, materialists aim to explain it as purely physical. Goff opts instead for the 1920s 'panpsychism' view, which claims that all physical matter shares consciousness.



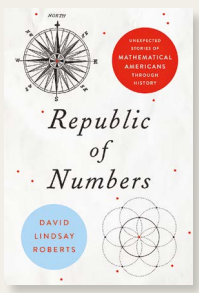
Imagination
Jim Davies Pegasus (2019)
Scientific books on creativity abound. But this deeply researched study of imagination — ranging from everyday practicalities such as planning a shopping list, to dreams and hallucinations — is not one of them. Cognitive scientist Jim Davies, who heads a Science of Imagination Laboratory in Canada, researches how to get software to replicate the processes our brains use to create visual scenes in our minds. But, as Davies admits, in psychology the jury is still out on whether "mental imagery exists as its own separate representation".



At the Edge of Time
Dan Hooper Princeton University Press (2019)
In 1919, when general relativity was confirmed astronomically, science knew nothing of cosmic origins. Even in the 1950s, Albert Einstein joked that "Every man has his own cosmology and who can say that his own theory is right!" Today, the Big Bang is universally accepted, and evidence suggests that gravity started to behave much as it does now within about 10^{-43} seconds. Yet much remains perplexing, explains astrophysicist Dan Hooper in this informed introduction to "the mysteries of our universe's first seconds".



The Imperiled Ocean
Laura Trethewey Pegasus (2019)
Three million US citizens work on the ocean — in fishing, oil and gas, tourism and other industries and services. The global figure is three billion. Journalist Laura Trethewey set out in 2015 on "an extended listening tour" to hear some of their stories. She describes a teenage Ghanaian refugee who crossed the Mediterranean, a 'water-squatting' Pacific Northwest community and a biologist who tracked the accelerating disappearance of the sturgeon. The vivid result — her debut — persuades us that "the ocean's story is also our own".



Republic of Numbers
David Lindsay Roberts Johns Hopkins University Press (2019)
This charming collection of 20 "unexpected stories of mathematical Americans through history" focuses not only on the greatest US mathematical minds, and includes just six career academics. Abraham Lincoln, self-trained as a surveyor, later studied Euclid — as demonstrated in his Gettysburg Address, "dedicated to the *proposition* that all men are created equal". A pity, however, to exclude Tom Lehrer, mathematician-cum-satirist, who composed the classic 1965 song 'New Math'. **Andrew Robinson**