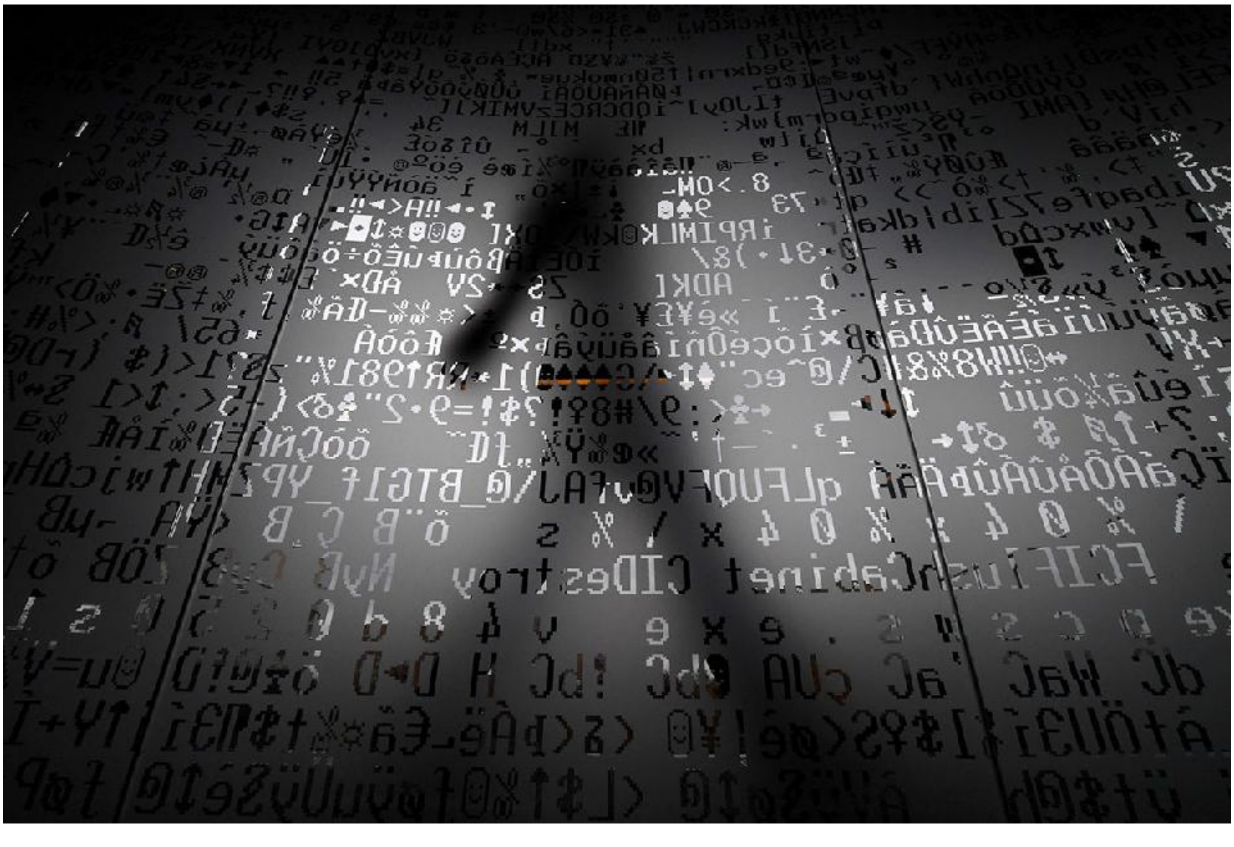
REVIEW 30 August 2017

The Darkening Web: Misinformation is the strongest cyberweapon

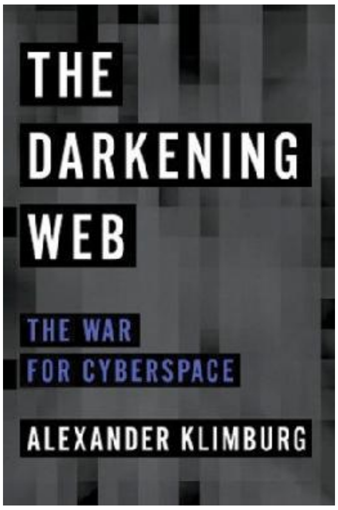
China watches what its own people say, Russia spreads its own version of events and the US brags. A new book shows that cyber-conflict is largely a war of words



Cyberwarfare attacks citizens' minds as well as their infrastructure
Kirll Kudryavtsev/AFP/Getty Images

By **Nina Jankowicz**

IN LATE June, I was leaving for a flight from Kiev's Boryspil Airport as news broke that Ukraine was the victim of another massive cyberattack. ATMs, gas pumps and supermarket checkouts were frozen. Government computers appeared to be seized by ransomware. Chernobyl's radiation monitoring system was affected. There were reports that the attack had grounded planes at the airport. Not that I could get there: I couldn't seem to catch a cab on a single ride-sharing app. The attack spread with frightening speed, but I eventually made it to Boryspil, where everything seemed to be functioning normally. Frankly, though, the thought of hurtling through the air in a metal tube guided by computers during a global cyberattack did give me pause.



It's this type of worldwide cyber-chaos – the type that could down airplanes, turn off respirators and plunge millions into darkness – that Alexander Klimburg warns of in *The Darkening Web*. And it's much closer to crippling our societies than world leaders would like to believe.

Deadly ignorance

Klimburg, a strategic analyst in this field, compares cyberwarfare to the threat posed by nuclear weapons. But there is one critical difference: while "the horror of the nuclear mushroom cloud [has been] burned into the minds of a generation of decision makers", there is little understanding within government, never mind outside it, of the consequences of all-out cyberwar. Without such a basic understanding, along with a more transparent policy, we risk being plunged into total cyber-conflict.

Having put the fear of God in us, Klimburg tells the story of the internet: how it was built and how it is governed – as a way of asserting US dominance, according to a few nations. He also talks about hackers, who are not the "400-pound guys" of President Trump's imagination, but complex beings who just as often work for governments as against them. We find out how they exploit the internet's vulnerabilities.

One of the key vulnerabilities in US cyber-policy, Klimburg says, is "cyber-innuendo". If governments were teenage boys, Washington would be the kid boasting about his latest escapades with the prettiest girl in class. His embellishments on a kernel of truth are meant to inspire shock and awe, but succeed in egging other boys on to sharing or pursuing even fiercer strategies of their own. Information about US cyber-dominance is established through strategic leaks, but these only serve to encourage actors like Russia and China to beef up their own capabilities and train their sights on the US and, increasingly, on their own people.

In China, for example, the Great Firewall "protects" citizens from problematic content, and political discussions are deflected by government contractors. Citizens' behaviour on social media is meticulously monitored and may soon be assigned a government "social credit score".

The Russian cyberthreat is, by contrast, meant "not to compete with the United States and the West, but somehow to catastrophically weaken them". Klimburg does a fine job explaining the various structures within Russia's security services that handle cyberwarfare. His definition encompasses not only the hacking to which the West has now grown accustomed, but also the widespread information warfare equally capable of influencing policy and populations.

Despite being well aware of the dangers of Russian information war, Klimburg falls victim to it, referring to the Russian invasion of eastern Ukraine as an "insurgency... and resulting civil war". This is exactly the narrative that Russia peddled after it invaded Ukraine's sovereign territory, sending troops, weapons and money to so-called separatists in the Donbas for three years, at a cost of 10,000 lives. With his knowledge of Russia, Klimburg should know better than to buy into this lexicon.

Klimburg's warnings regarding Russian cyber-aspirations, however, are on the money. He does not think the US election was turned around solely by Russia's campaigns and incursions. Still, his recommendations might have helped the Obama administration retaliate while evading charges of partisanship. Klimburg argues that governments should be clear and transparent about what types of cyberattacks they face and what "deterrence by cyber-means" should entail.

"In China, behaviour on social media may soon be assigned a government 'social credit score'"

Time treats books in strange ways. Seven months into the Trump administration, which is actively working to unravel the freedom of the internet and aiding the spread of disinformation from the Oval Office itself, *The Darkening Web* feels less like a work of advocacy, more like a cry for help. If only we had known, perhaps we could have staged an intervention.

The Darkening Web
Alexander Klimburg
Penguin Press

This article appeared in print under the headline "Ending the world with a nod and a wink"

Nina Jankowicz is a foreign affairs specialist based in Washington DC

Magazine issue 3141, published 2 September 2017