Book review: "The Darkening Web: The War for Cyberspace" by Alexander Klimburg

Alexander Klimburg’s ‘The Darkening Web’ warns the internet is already being exploited by nations

By Glenn C. Altschuler   Aug 13, 2017
Penguin Press, $28

In 2014, 61 percent of the 1,600 experts polled by the Pew Research Center stated that a major cyberattack causing significant harm to a nation or nations was likely to occur within the next decade.

Alexander Klimburg, a program director at the Hague Centre for Strategic Studies and an adviser to governments and international organizations on cybersecurity strategy and internet governance, agrees that the risk of a cyberwar is many magnitudes higher than a nuclear war. In “The Darkening Web,” Klimburg provides an extraordinarily informative and accessible examination of the threats to physical infrastructure, privacy and the free flow of information posed by the struggle for control of cyberspace. Ripped from yesterday’s — and tomorrow’s — headlines, “The Darkening Web” shines spotlight on a vitally important and little understood threat.

By design or through carelessness, Klimburg claims, the United States and other nations tended to leave the internet alone during its formative years, enabling it to establish trust and user autonomy as core attributes.

As the internet became a necessity for modern societies, however, governments have sought to exploit it for political purposes. Seeking to break what they perceive as the cyber dominance of the United States (where the internet was born), Klimburg indicates, authoritarian governments have increased attacks on infrastructure, industrial espionage and “informational effects” on their citizens as well as their enemies.

Klimburg describes Russia’s cyberattacks on the infrastructure of Estonia, Georgia and Ukraine. He documents Russian dissemination of fake news — and the hacking of America’s Democratic Party emails in 2016. And Klimburg notes how Russian President Vladimir Putin has used revelations about the Stuxnet virus (that disabled Iran’s nuclear program) and Edward Snowden’s disclosure of National Security Agency operations to charge the United States with cyber hypocrisy.

Klimburg also explains why China has curtailed its theft of economic data and intellectual property from the private sector. At the same time, he reveals, the relative freedom of Chinese citizens online is deteriorating. To maintain social stability, for example, the government recently proposed a chilling “social credit score system.” Supported by data mining of blog posts, social media contacts and purchases, the system would reward good behavior (praise of the government policy) with, say, easy access to travel permits, and punish bad behavior (posted comments on the Tiananmen massacre).
Bad behavior will intensify, Klimburg warns, if the plan, introduced by Russia and China, to establish national sovereignty over the internet, is adopted. Instead, Klimburg advocates keeping the principal cyberspace dimensions — international peace and security; the economy and crime; and governance — separate. He envisions a role for the United Nations in the first two domains and recommends a “multi-stakeholder” approach to governance, with participation by government officials, the private sector and members of civil society.

Like climate change, Klimburg emphasizes, cyberspace presents a potential “crisis of the commons.” He hopes his “crash course introduction into this new dimension of human conduct” will stimulate “netizens” to lobby for the collective good. At stake, he concludes, apocalyptically but perhaps accurately, is the future of democratic societies.

Glenn C. Altschuler is the Thomas and Dorothy Litwin Professor of American Studies at Cornell University.