Review

Reviewed Work(s): Nanoweapons: A Growing Threat to Humanity by Louis A. Del Monte

Review by: Patrick M. Milott

Source: *Strategic Studies Quarterly*, Vol. 14, No. 1 (SPRING 2020), pp. 142-144

Published by: Air University Press

Stable URL: https://www.jstor.org/stable/10.2307/26891888

Director of National Intelligence James Clapper's opinion, impacted central cybersecurity tenets by undermining the confidentiality, availability, and integrity of federal data involved in verifying US federal employees' financial, personal, and security clearance files (361). The three OPM attacks, months apart, each targeted different network systems. OPM's recovery process eventually discovered one piece of installed malware per device, and no attack was discovered until three weeks after the last. Carlin clearly shows that despite the US government's own cybersecurity focus during the relevant time periods, federal agencies failed to meet their own standards for commercial industry. A 90-day cyber-defense improvement sprint in 2015 resulted in only 15 of 29 agencies meeting basic cyber security requirements (365). After 10 years of Carlin's assistance directing policy and legally pursuing adversaries, evidence indicated that barely 50 percent of federal agencies complied with even the most basic preventative measures.

There is some new material about US actions against foreign cyberattacks, but uncovering Carlin's own role was difficult. His appearance seems perfunctory and based on personal connections rather than contributing activity. For example, the Russian-oriented "Slavik" chapter does not include a single action by Carlin. The standard for authors recounting personal actions in their government service—if not a full biography—should be compilations similar to Juan Zarate's *Treasury's War* (2013), describing the Department of Treasury's counterterrorist financial actions. Carlin does possess considerable personal knowledge as a recently departed federal official, though the text fails to convey any sense of urgency or immediacy that he feels toward these struggles from his own experience. The overall conclusion makes a perfunctory mention of a "code war," the need for increased training, and carrying American values onto the Internet—all good ideas but lacking connection to earlier material. Carlin's text offers some learning, but any emphasis on the Justice Department's unique influences unfortunately are absent.

In general, *Dawn of the Code War* provides an adequate introduction to the last decade's cyber activity, especially those in the gray zone of not-war, faced by the United States. Cyberspace novices will get a substantial grounding while more advanced readers may find some interesting nuances about previously studied attacks. Carlin and Graff manage to advance the field somewhat with compiling significant information under a single cover to create a worthwhile stop. The text jumps somewhat chronologically but not to such an extent as to make following the material difficult. Long for an individual account at 400-plus pages, the book reads quickly. I found the material mildly entertaining and beneficial overall. While this work is not my first suggestion to pursue for a cyber history, I recommend that new cyber students add it to their bookshelves and more experienced students consider *Code War* for their backlog. An improvement would be a future work from Carlin depicting his own experiences in greater detail.

Dr. Mark T. Peters II, USAF, Retired

Nanoweapons: A Growing Threat to Humanity by Louis A. Del Monte. Potomac Books, 2017, 244 pp.

When new technologies cross from industry to the battlefield, calls arise to slow the process and consider international implications of using these weapons. Louis A. Del Monte's *Nanoweapons* is one of those calls. A physicist and former executive at IBM and Honeywell, Del Monte led advancements in microelectronics and sensors. His work is a serious attempt to use publicly available information to address the development and use of nanotechnology as weapons. The author brings together ideas normally relegated to science fiction (e.g., laser weapons, artificial intelligence, and self-replicating nanorobots) and uses his technical background to inform the reader as to what is science fact. While his most alarming predictions for humanity's survival project to the year 2050 and beyond, he argues that his concerns are timely. He indicates that while revolutionary military nanotechnologies (e.g., stealth aircraft) may take decades to field, they are nonetheless currently being developed. Now, according to the author, is the time to discuss the dangers of nanoweapons.

The author's main thesis is that nanoweapons are a danger to humanity that demand greater attention. Despite the secrecy surrounding the development of nanoweapons, Del Monte is confident of their threat. This fear is based in part on the ranking of nanotechnology weapons by the Global Catastrophic Risk Conference at the University of Oxford as the most probable means to cause human extinction by the end of this century. Examples of nanoweapons discussed in the book include nano-enhanced lasers, smaller munitions with increased explosive force, and self-replicating smart nanorobots (SSN). SSNs search for and destroy targets without human input and self-replicate with materials found in the environment. According to the author, SSNs are gravely dangerous nanoweapons that humanity should prohibit. Central to his concern for humanity's survival is what he sees as the inherent difficulty in mounting defenses to nanoweapons given their capability to avoid detection and the ability of those who use these arms to escape attribution. While considerable resources have been dedicated to countering nuclear weapons, little is publicly known about protection from nanoweapons. This is especially concerning to the author because some nanoweapons have characteristics similar to biological pathogens. Giving his readers reason to be apprehensive, Del Monte turns to explaining how today's nanotechnology can be used to create nanoweapons.

While nanotechnology is already improving our computers, sunscreens, and building materials, the first section of the book provides the nontechnical reader an easy-to-understand introduction to nanotechnology and how it may be used in arms development. The author organizes nanoweapons into five categories: offensive strategic, defensive strategic, offensive tactical, defensive tactical, and passive. Examples are provided for each category, along with an explanation of its offensive, defensive, or passive nature. For instance, the offensive strategic category includes artificially intelligent nanorobots that can target particular individuals, hypersonic glide missiles (whose development will rely on developing certain nanomaterials), nano-enhanced fuels, and nonelectric guidance systems. The other categories include additional guidance for organizing nanoweapons. While readers will find these categories helpful, a workable definition of nanoweapons is missing.

With this deep level of organization dedicated to understanding nanoweaponry, the reader would hope for a more useful definition of nanoweapons. *Nanoweapons* are defined in the book's glossary as "any military technology which exploits the use of nanotechnology" (229). Although this definition will capture all nanoweapons, it will also include many items that are not weapons. This definition would include a military finance office using a publicly available desktop computer with a nanomanufactured microchip. Is building a weapon with nanomanufactured components all that is required to make the weapon a nanoweapon? If a dry-docked ship is sprayed with anticorrosive nanocoating—increasing its hull strength tenfold (as an MIT study referenced in the book suggests)—is the ship now a nanoweapon? The book makes clear that nanotechnology is an enabling technology that will empower a wide range of civilian and military applications. But it does not wrestle with the problem that an SSN is fundamentally different than an anticorrosive nanocoating. This issue of defining nanotechnology is a common attribute of nascent scientific fields, but the reader is nevertheless left wanting more. Without addressing this definitional problem directly, Del Monte instead uses other methods to discover what nations are emerging as nanoweapon leaders.

He categorizes the factors needed to facilitate nanoweaponry development and sorts nations by these factors into the Nanoweapons Offensive Capability of Nations (NOCON) list. The most powerful group, nanoweapon nations—such as the United

States and China—has the ability to commercialize nanotechnology, possesses a national desire to strengthen its militaries, and demonstrates an ability to partner with other leading nanotechnology nations. Del Monte goes on to mention other nations on his NOCON list, all of which have varying interactions with nanotechnology. Giving the reader reason to be concerned for the international implications his NOCON suggests, he then highlights the events that may tip us into a nanoweapon-driven war.

He predicts two singularities that will spawn nanoweapon-related international disruptions. In addition to the creation of SSNs, the other singularity is the advent of artificial intelligence (AI) that will exceed human intellect. AI will solve many of humanity's greatest problems, the author posits, but it will also create better SSNs. If AI and SSNs are combined, alliances will form to maintain advantages in a new cold war around the development of AI-powered SSNs. Given their importance, international power will then be rebalanced around nanoweapon capabilities. Nuclear weapon use will increase since nanotechnology will empower their miniaturization and reduce their fallout. It is these disruptions, brought on by the AI and SSN singularities, that Del Monte claims will dramatically increase the chance of human extinction by 2100. Given this pessimistic prediction, *Nanoweapons* next discusses reasons for hope.

The author maintains some optimism for humanity. He notes that humanity has engaged in conflict since the beginning of our existence, but recent developments, such as the Treaty on the Non-Proliferation of Nuclear Weapons and the Biological Weapons Convention, show that humanity can act to prevent its extinction. Once humanity comes to know the existential threat that nanoweapons represent, humanity will act to limit their use and thus avert disaster. What we recognize when we use a new personal computer, he argues, is not the nanotechnology enabling its use but the impressive performance it achieves. The author states that humans understand technology by its function, not the technology itself. Thus, to forestall the need to demonstrate a nanoweapon's threat to humanity, he indicates that current treaties and conventions concerning weapons of mass destruction should also regulate strategic nanoweapons.

A workable and more precise definition of nanoweapons will improve this area of study by allowing policy makers to grapple with nanoweaponry development. It will empower leaders to specifically categorize an adversary's capabilities and document who is developing nanoweapons with greater specificity. Assuming that Del Monte's catastrophic predictions are accurate, more scenarios are needed to better inform technologists, military commands, and national leaders working on ways to prevent the negative implications of these technologies. This work is worth reading because it ties together the technical, political, economic, and practical challenges associated with nanoweapons. The initial portion of the book is especially worthwhile for those seeking an approachable introduction to nanotechnology and its use as weaponry. Suggestions for additional reading in this area of futurism are Peter W. Singer's *Wired for War* and Michio Kaku's *Physics of the Future*. Strategic leaders will appreciate the discussions on organizational problems associated with fielding nanoweapons and rebalancing international power. Tactical leaders will find themselves working through different ways to use and defend against nanoweapons. Finally, fans of science fiction will appreciate a technical introduction to many real concepts previously relegated to fantasy.

Maj Patrick M. Milott, USAF

Unrivaled: Why America Will Remain the World's Sole Superpower by Michael Beckley. Cornell University Press, 2018, 248 pp.

Graham Allison's concept of the Thucydides Trap has fed the hubristic notion in polarizing policy debates that China's rise in the world is in relative proportion to America's