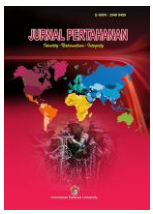
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



BOOK REVIEW
POWER TO THE PEOPLE: HOW OPEN TECHNOLOGICAL INNOVATION IS ARMING TOMORROW'S TERRORISTS

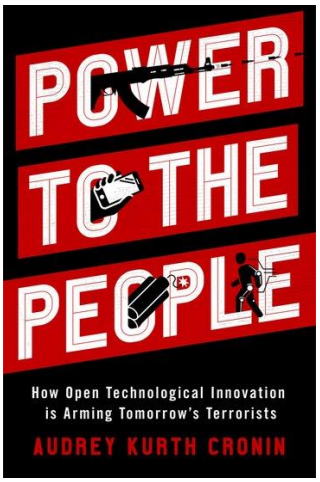
Rangga Amalul Akhli
Indonesia Defense University
IPSC Area, Sentul, Sukahati, Citeureup, Bogor, West Java, Indonesia 16810
ranggaamalul@gmail.com

Article Info

Article history:
Received : June 19, 2021
Revised : November 1, 2021
Accepted : December 20, 2021

Keywords:
Asymmetric Warfare,
Audrey Kurth Cronin,
Power to the People,
Technological Innovation,
Terrorism

Book Info



Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, Oxford University Press 2020, 440 Pages, 6-1/8 x 9-1/4 inches.
ISBN: 9780190882143

DOI:
http://dx.doi.org/10.33172/jp.v7i3.1260

It is commonly known that the terrorism issue has become one of the contemporary security challenges a state and its strategic planners should encounter. In most cases, strategic planners' focus is to identify a group of terrorism doctrine and motivation. The roots of it can be classified at least by the feeling of injustice, mental illness, radicalization, or misleading ideologies. In literature, there have been a lot of authors in terrorism books that provide brilliant arguments explaining the existence of terrorism. Amid such numerous books on the subject, nevertheless, it seems like there is a missing link as authors rarely discuss comprehensive explanations regarding how the terrorist is armed. This question is essential since terrorism cannot do such attacks if they do not possess the means to do that. Audrey Kurth Cronin's book attempted to fill this gap by providing in-depth historical studies and drawing potentially complicated situations as states cannot seal the weaponization process of the terrorist group.

Cronin's thesis is to state that in an era in which a new breed of technologies is continuously appearing in a fast time,

technologies usages possess a critical point to become new potential dangers as terrorist organizations are likely to utilize them for violent purposes, wreak havoc and destabilize state security. Therefore, states should master this issue and formulate an effective asymmetric warfare strategy to minimize security vulnerabilities from any kind of irresponsible use of disruptive technologies by terrorist organizations.

In general, this book consists of three parts within which Cronin set for theoretical frameworks for the book in part 1; followed by the history of technological innovation in weapons which is misused by the terrorist group in part 2; and in the final part, it discusses the latest developments of technological innovations, and how terrorist groups take advantages from the current inadequate policy.

In part 1, Cronin elaborates the works of prominent scholars to explain the relationship between war and technology and how states are secured from the source of threat. Cronin begins with Max Weber's theory regarding states' monopoly use of force. According to this theory, states would increase sophisticated lethal technology capabilities to affect war and confer power because it is believed that states' military innovation superiority determines the result of war.

For instance, during the Matabele War in 1893, using Maxim Guns, a 700-man of UK force wiped out 1500 Matabele King warriors. Another example is manifested by the Battle of Midway 1942 between the Japanese Navy against the United States and its allies. Because of the excellence of the American cryptography system, the US won the battle although at that time the Japanese Navy had more deployed forces. Japan lost four carriers and two cruisers meanwhile the United States lost a carrier and a destroyer with a casualty ratio of about 10:1. The invention of nuclear has further developed another strategy to secure from direct military attack as it has a credible deterrence effect. However, as the adversaries are to include non-state actors, all of the possession of innovative military technology cannot automatically assure the security of states.

The world now is entering the fourth wave of violation characterized by the rising of religious fundamentalism influence. Islamic States, Al-Qaeda, Shiite Hezbollah, Jewish Kahane Kai, Japan's Aum Shinrikyo among others represent the violent groups during this wave. Previously, the world has recognized the trend of anarchism, ethnonationalism/separatism violence, and Marxism ideology-based movement. Through those four waves, it is understood that terrorism tactics can be made through bombings, hit and run attacks with small arms such as AK47 assault rifles, hijacking or kidnapping, to suicidal attacks through lethal explosive weapons. The new digital tools of the internet help groups attract new followers and mobilize them.

Cronin also argues that terrorist groups in their development can innovate everything to be their source of weapons. She explains it extensively in part 2. Starting from Narodnaya Volya that assassinated Tsar Alexander II through the misuse, accessible, and cheap dynamite whose primary purpose was designed for construction and mining at that time. And then, for another case, the Irish rebellion movement against the UK government. Helped and funded by the Irish who were exiled to the US, they learned how to build an explosive bomb themselves. Moreover, they could innovate their signature by combining an explosive, a detonator, and a time delay unit.

Among other things, the AK47 has also become another trademark in terrorist organizations. In this part, Cronin explained it extensively from Soviet use to the current dispersed use that armament factories to produce the AK47 can be found in many states, such as Ukraine, India, China, Nigeria, Iraq, and many more. Some vendors make illegal deals with terrorist organizations.

In the final part, Cronin explains the role

of current technological development to support terrorist organizations. There are numerous intriguing and important data here to understand how the terrorist is armed in the internet era and why some policy of states is ineffective. In this part, she first argues that terror attacks can be inspired by the spread of hate speech through multiple media, be it magazine, or online-based. Anwar Awlaki can be the best example of why someone wants to be a terrorist and arm him/herself.

Despite having passed away, his hate speech could still be watched on YouTube or Facebook. the US government blocked internet content regarding Awlaki, but his follower could still find it. Even he gained more influence after his death. Several terror attacks in the US, Singapore, Bangladesh, and the UK from 2013-2016 exposed evidence that there are linkages between attackers and Awlaki teachings. Simply put, the internet has facilitated terrorist mobilization to do such violent acts. Agitators connected to the internet use this kind of teachings to increase the means of mobilization besides the spread of offline pamphlets, books, newspapers, and many more.

To reinforce her argument that the internet matters in arming and part of psychological tactics of terrorist, Cronin point out terrorist organization in the Middle East. She notes that IS (Islamic State) has utilized Twitter as its marketing campaign in 2014. In Iraq, this campaign was considered effective in toppling down the Iraqi Government and society through the spread of violent photos and videos of executed Iraqi soldiers posted on Instagram and Twitter. Many Iraqi soldiers took off their uniforms, dropped their weapons, and joined the civilians leaving the region. Other terrorist organizations have also utilized the same strategy on the internet, such as Al-Shabaab, Al-Qaeda, and Boko Haram. Besides spreading hatred, manipulating targets on their narratives, and creating fake accounts on social media to assist their agenda, terrorist organizations simulate the creation of bombs with dozens of different language instructions. Some tried to erase them, but the internet always provides terrorists with alternative ways. Therefore, it is true as Cronin argues that this dark side dimension of internet connectivity should therefore be anticipated by governments to prevent further mobilization and radicalization on the internet.

The book also notes that in the Middle East, religious fundamentalism-based terrorist organizations are considered to be the more extreme version and possess more advanced technologies than those outside the region. Here, they have operated weaponized drones (UAV/Unmanned Aerial Vehicle). Iran is considered to become a state provider that gave this technology to several organizations, such as Hamas, Hezbollah, and Houthi rebels until the internal component of these organizations could independently build their drones to attack their political opponent.

Drones are considered impactful not only for attacking but also for surveillance purposes. Cronin provides another important piece of data regarding the United States' experience in operating drones to track terrorist presence. From Cronin's point of view, the use of drones provided other issues in the United States' war on terrorism. The drone market is now dominated by China-based company, Da-Jiang Innovations (DJI) and the U.S. army operated it due to its impressive yet inexpensive. The issue is that every time a DJI system is launched, it sends a pingback to the manufacturer. Therefore, whenever the Islamic State of Iraq and Syria (ISIS) or the U.S. Army, or various other actors use these off-the-shelf systems, data about their activities is captured and aggregated in DJI's massive commercial database. By 2017, sensing the dangerous effect from the DJI, Lt. Gen. Joseph H. Anderson, U.S. Army deputy chief of staff ordered to terminate this kind of drone.

Cronin also depicts that the popularity of

drones also occurs in IS and some separatist and proxy groups in Ukraine. IS militia experiment has been successfully developed weaponized drones and commercialized them. In a month by 2017, IS could launch the aerial attack from drones from 60 to 10 times in Iraq and Syria, intimidate and kill society. Iraqi force operation later had also confirmed that they found IS headquarter dedicated to transforming commercial drones such as China DJI Phantom into the weaponized drone.

The drone is used also in a proxy war between Ukraine-Russia. Russian forces routinely dropped bombs from the UAV. Here, another instrument of arming terrorism is highlighted by Cronin. She argues that the source of armed terrorists can also be based on crowdfunding. In the Ukraine conflict, for instance, some Ukrainian diaspora jointly provided cash to finance the purchase of drones. The reason why drone was chosen is that, again, it is cheap, cheaper than having to buy fighter jets or missiles. The drone is also modifiable and easy to be armed with.

In the last chapter, Cronin reminds us that the possession of artificial intelligence (AI) can also be the source of terror. AI may be expensive in its development, a terrorist organization may also not afford it. However, as stated above, there is a possibility that the organization is used as a proxy by certain states. There is a possibility that they will provide certain technologies for terrorist organizations. When AI gains popularity in conflict, the outcome of conflict may be hard to predict. Some AI can also be used as an information manipulator that can also threaten stability. We also have to be concerned with AI, because the use of robots may displace human works. If policymakers cannot find effective solutions, there must be greater economic inequality and encourage violence further.

To conclude, I think this book has delivered so depth and extensive understanding of terrorist attack history with its relations to the technological adaptation. By reading this book, decision-makers and strategic planners can prepare a more concrete policy to encounter terrorist and separatist attacks.

However, the book left me incomplete and gave some other thoughts. While many elements of Cronin states had occurred in Indonesia, such as bombing methods, crowdfunding, self-radicalization through the internet, or illegal arms sales, there is one critical element that remains to be explained. In this regard, it is about why drones have not been utilized as terrorist and separatist group instruments of attack in Indonesia? This puzzle might be one critical point on Cronin's theory of technological adaptive terrorists. As we know, a drone can be bought easily for the past few years. I do not expect that terrorists utilize it here in Indonesia anyway. Nevertheless, at least since the Bali bombings two decades ago, there have been no significant changes in terrorist and separatist attack patterns. Drones are not used although drones can become the next differentiator.

More importantly, this puzzle happened in a time of the abundance of information on the internet. Theoretically speaking, there must be easier for them to learn and assemble armed drones but they do not strategically utilize this idea, leading to another cynical question of whether they are truly adaptive to the invention of technologies. Therefore, further investigation into this puzzle might be important. The next research agenda to explain the causality of this puzzle might be important for the strategic studies literature or terrorism studies in particular.