Advanced Conventional Weapons and Emerging Technologies: Recognizing and Preempting Proliferation Threats

ANDREA VISKI, Ph.D
FEBRUARY 2022

Introduction

The proliferation of advanced conventional weapons (ACW) poses a grave threat to international peace and security. The acquisition by a growing number of countries of sophisticated advanced weapons systems follows a trend whereby the potency of specific ACW systems is compounded by integrating emerging technologies, such as artificial intelligence/machine learning or robotics.[1] Whereas the hardware – the equipment, materials, and components – for these systems can be manufactured indigenously or imported, access to and acquisition of ACW-related emerging technologies is a more daunting challenge. To mitigate the ACW proliferation threat, countries must develop strategies to recognize, preempt, and counteract malicious technology acquisition.

This article will analyze the threat of ACW and emerging technologies by describing acquisition typologies and the challenges they pose for targeted countries and sectors. The article will link these typologies to preemptive measures that governments and their technology holders can take to prevent malicious acquisition.

Typologies of ACW Technology Acquisition: Challenges

Traditional defense and dual-use export licensing systems are built to impede the spread of ACW-related tangible goods to proliferator states. In many cases, the hardware itself is already available – for example, many states already possess Maneuverable Reentry Vehicles (MaRVs), a type of ballistic missile whose warhead is capable of autonomously tracking ground targets.[2] However, the development of hypersonic glide vehicles, which integrate technologies that make the vehicles harder to detect, track, and prevent attack, require technology research and development that is not within immediate reach of countries embarking on development programs.[3] Acquisition of

[1] Other technologies often identified as "emerging" or "disruptive" include big data analytics, internet-of-things, virtual and augmented reality, smart sensors, additive manufacturing, robotics, novel/smart materials, quantum computing and encryption, semiconductors, and energy capture and storage technologies.
[2] China, France, India, Iran, Israel, Pakistan, Russian Federation, United Kingdom, United States.
[3] "Hypersonic Weapons" Background and Issues for Congress," Congressional Research Service, October 19, 2021, <https://sgp.fas.org/crs/weapons/R45811.pdf>.

technology – the intangible, yet critical component of many advanced weapons systems – is more difficult for national governments to monitor and control.

The strategies countries employ to acquire sensitive emerging technologies for integration and development of their ACW programs varies. Straightforward investment into national R&D programs remains crucial. Beyond that, acquisition can take both licit and illicit forms. Examples of licit acquisition include academic and research student exchanges, repatriation of technology experts, joint ventures, international investment and acquisitions, and open-source information collection.[4] The area where less global attention is directed, but that presents a significant proliferation threat, is illicit technology acquisition. More obvious examples of this activity include cybertheft or espionage, but in many cases, academic and student exchanges and interactions are exploited to reach proliferation objectives. Because these typologies are less straightforward than acquisition of tangible goods, less resources generally exist within national systems to preempt and counteract them.

Acquisition of technology through foreign direct investment (FDI) is another concerning typology where the technologies being acquired could have uses in the ACW context. In most cases, though the acquired organizations' technologies seem only to have civilian uses, they do in fact have military uses, as well. For example, foreign acquisitions in automotive industries, specifically in technologies such as remote occupant sensing or human-machine interface technologies, could be considered for review due to the technologies having potential military applications (i.e., human-machine interface technologies can allow humans and machines to interface better in a military setting). Even in sectors that have more obvious defense links, such as aerospace, or specific emerging technology companies in areas like emotional analytics or gesture control, sensitive technologies could be acquired absent appropriate review procedures for FDI.

The common characteristic between typologies of ACW-related emerging technology acquisition is the relative lack of national and organizational measures to preempt and counteract it. In most cases, national export control systems cover both tangible and intangible goods, yet governmental

[4] Tate Nurkin, "China's Advanced Weapons Systems," Jane's, May 12, 2018.

resources for outreach and awareness-raising focus on exporters – mainly private companies – of materials, equipment, and components. Indeed, enforcement also focuses on tangible goods, through cooperation with Customs, border security, intelligence, and other enforcement agencies. However, to effectively counter the threat of ACW-related technology acquisition, governments must develop strategies and take action to raise awareness and strengthen compliance within sectors targeted for technology acquisition, such as research institutes, universities, and non-export-controlled emerging technology sectors.

Recommendations and Conclusion

The threats posed by ACW proliferation and the associated technology acquisition by malicious actors can be mitigated through greater awareness of specific vulnerabilities and resources directed at preempting technology theft. While a myriad of potential actions could be taken, the following recommendations represent some of the most basic, universal best practices countries can consider in response to ACW technology malicious acquisition:

- Identify organizations that are technology holders and maintain an updated national database;
- Develop outreach to key organizations to raise their awareness of proliferation threats. Note that outreach strategies should be tailored to the specific audience, which will differ from private sector exporters of tangible goods;
- Encourage technology holder organizations to develop Internal Compliance programs that ensure that all individuals in the company are aware of technology theft risks and how to recognize them, and what to do in response;
- Develop national-level red flags that organizations can use to recognize technology theft;
- Establish review procedures for Foreign Direct Investment;
- Develop a robust inter-agency information sharing system to develop the capacity to receive timely and accurate information regarding acquisition threats;
- Participate in regional and international activities to develop cooperation, learn best practices, and develop regional responses to acquisition threats.

States must recognize that the threats posed by ACW will remain, and that the potential of emerging technologies to enhance the power of these advanced systems presents a unique problem that requires innovative and proactive solutions. Through robust public-private cooperation, as well as specific measures to preempt and counteract malicious technology acquisition, states can play a critical role in strengthening international peace and security.