*Alliances and the Transfer of Cyber Weapons*

Lt Col Randal Allen, US Air Force

The Cyber Era

Prof. Eviatar Matania

25 March 2020

Introduction

The imperative for international cooperation in fighting cyber crime and cyber terrorism and even defending against state-sponsored cyber warfare is well founded. However, very little has been written about the need for international partnerships in offensive cyber operations. Alliances and coalitions can provide untold benefits in the large-scale use of kinetic offensive force, so it is worth exploring how partnerships can be effectively used in applying cyber force. As much of long-term international defense partnership is promoted by weapons sales and the use of common military platforms, the following analysis will rely on weapons sales as a tool for developing some ideas for cyber partnerships in conducting offensive activities. We will begin by exploring the role of traditional weapons sales in national security, then discuss how cyber weapons are different. Next, we will look at what benefits are to be gained by transferring cyber weapons, and then we will conclude by discussing the best circumstances for such sharing.

Role of Weapons Sales in National Security

The economic benefits to weapons sales are obvious and might easily distract the novice national security analyst away from the defense benefits. Certainly, the high-tech nature of today’s weapons and the size of the market ($67.9 billion in 2019 US sales - (Mehta)) is indicative of their economic importance. A 2017 sale of F-15 fighter aircraft to Qatar, for example, was reported to have created 60,000 American jobs (Boeing Wins $6.2 Billion Qatar Contract for 36 F-15s). Additionally, many important technologies in use outside of the military had their genesis in defense research and development. Further, many arms producers, such as aircraft builder Boeing, also produce similarly high-tech goods for the civilian market. For example, Boeing is also America’s top competitor for civil aviation sales, and no doubt its export of military aircraft helps its ability to offer the best product in overseas civil airliner competitions.

In addition to these economic benefits, weapons sales have an even greater impact on the defense pillar of national security, and thus offer a prime means of boosting national power. High-end weapons producers, such as the United States and Russia, are able to extend their military superiority to their security partners by exporting these advanced systems. As long as patron-client security interests remain aligned, these sales can act as a force multiplier for the producing country. For example, Jordan and the United Arab Emirates both employed their US-produced F-16s in combat operations over Libya and operations to defeat the so-called Islamic State, hitting targets assigned by the US-led planning teams. In addition to the diplomatic benefits of having these two Arab countries actively participating in coalition operations, this arrangement allowed the United States to achieve the same military effects as it would gain by employing more of its own aircraft and munitions.

Weapons sales to client states may also create a stronger dependence on the patron, ultimately increasing the patron’s influence over the client. The decision to buy a new fighter aircraft is a significant one, not least because of the cost of the aircraft themselves, but also the high financial cost of associated weaponry, training and infrastructure. Additionally, purchasing countries often must adapt their force structures to best absorb and operate these aircraft and their associated systems. These commitments bind the purchaser to the producer for decades of after-sales support, munitions replenishment, and upgrades to both training and the equipment itself. All US Government-managed weapons sales, known officially as Foreign Military Sales or, simply, “FMS,” are governed by contracts stipulating that the weapons will be used only in “legitimate” self-defense or in furtherance of UN-sanctioned military activity. Consequently, the United States has used the threat and actual withholding of follow-on support to apply political pressure on its weapons buyers. The success rate of such pressure tactics has been disputed (Rounds), but it remains an attractive reason to win a sale over other producers.

Weapons sales can also be leveraged to expose vast numbers of the buyer’s military personnel to the producer’s nationals, its own country, and its way of life. The United States methodically takes advantage of the resultant opportunities to wield soft power. The typical purchase of a new American fighter aircraft platform often involves the exchange of thousands of personnel throughout the lifetime of that aircraft, which can last for more than 40 years. This can include training hundreds of the buyer’s aircrews, maintenance, and support personnel. The US Defense Language Institute-English Language Center (DLI) at Lackland Air Force Base, Texas, exists solely to teach foreign military members English in preparation for their technical training on US weapons systems or professional education at American military institutions. DLI deliberately maximizes these trainees’ exposure to American culture via field trips and the assignment of a sponsoring American family in order to foster a favorable attitude towards America and Americans (Warren).

Selling advanced weaponry also provides opportunities to reduce the unit cost for the producing country’s military. US law stipulates that original, non-recurring research and development costs for major weapons systems must be passed on to FMS buyers (Non-Recurring Costs and Waivers). Today, budgeting for the development of many new US weapons systems is accomplished with FMS in mind and the F-35 was planned from the beginning to be a multi-national effort, with costs spread to many buyers. Additionally, sales provide opportunities for the selling country to make improvements based on performance information gleaned from buyers’ employment of these systems in combat. For example, Israel employed the F-15 in combat extensively over Lebanon beginning in 1979, whereas the American F-15s had not flown combat missions until Desert Storm in 1991. It stands to reason that the United States would be able to leverage the Israelis’ combat experience in the F-15 in the interim.

Cyber Weapons

Can the same benefits be achieved with the sale or sharing of cyber weapons? In order to answer that question, it is first necessary to explore how cyber weapons differ from traditional weapons and what the implications could be of sharing cyber weapons amongst international partners. Perhaps the most obvious difference is the very real danger of proliferation. Unlike nuclear, biological, and chemical weapons, which require vast facilities and, in the case of nuclear weapons, fissile material, cyber weapons can be pirated like any other software (Hedge). Presumably, copy protection measures could be built into the design of cyber weapons, as they are in today’s software applications. A “registration” process might be required in order to prevent the use of any weapon until notice has been sent electronically to the exporter, who then approves before it can be employed. Similar measures might also be utilized to place a time limit on the viability of any given cyber weapon. Such a restriction might prevent the importer from using the weapon in a manner inconsistent with end-use agreements in place with the exporter. For example, the United States might sell a cyber weapon to a Persian Gulf state for use against Iran in an open military conflict. Presumably, the United States would have strong objections to that weapon’s use in a separate conflict to which it is a neutral party or a supporter of the opposite side. End-use agreements are standard in all US sales of major traditional weapons (Kaidanow). Using the techniques described above, cyber weapons are likely easier for the exporter to control than traditional weapons. End-use violations are a major concern for the United States, which provides weapons to the UAE and Egypt, both of which are aligned with Russia in opposition to the US- and UN-supported government in Libya (England). Proliferation of US-supplied weapons is also an American concern, and there is always a risk of importers re-transferring them to unauthorized entities (Elbagir, Abdelaziz and Abo El Gheit).

Indeed, the potential damage from a lost cyber weapon can far exceed that of a bomb or missile. The leak of cyber weapons at the NSA led to the NotPetya attacks, for example, which resulted in over $10 billion in worldwide damages and multiple hospitals having to turn away patients (McQuade). By sharing these weapons, the exporter multiplies its risk of even an unintentional leak. With both the CIA and NSA having experienced their own losses of cyber weapons, whether at the hands of a disgruntled employee or one with poor cyber hygiene, special consideration would have to be taken before an export should be approved. At a minimum, safeguards would have to be built in such that only the compiled applications are available to the importers and not the source code, which could be manipulated and misused.

Sharing cyber weapons also exposes the exporter to the risk of misattribution should the target identify “fingerprints” on the weapon and mistakenly trace the origin of the attack back to the exporter. Worse yet, the importer might purposely use the weapon in such a way as to falsely incriminate the exporter in order to carry out a false flag operation. Presumably there are countermeasures that can be adopted, though not without diminishing the weapon’s value. Despite developers’ best efforts to avoid leaving fingerprints behind, it often happens, and so exporters cannot rely on careful coding alone as the solution to avoiding misattribution. Therefore, any end-use sales agreement should include provisions for purposely incorporating signatures of the importer. However, a major benefit of using cyber weapons over their kinetic counterparts is plausible deniability, so a weapon with such signatures built in would have a greatly reduced value.

Finally, cyber weapons can lose a great deal of their potency once “fired” even once and so exporters should think twice before providing their most advanced and precious weapons to their partners. The nature of cyber weapons is such that they take advantage of unknown vulnerabilities, so if an exporter provides a tool for use against a mutual adversary and the importer were to employ that tool, the adversary would very likely be able to identify the vulnerability exploited and patch it. Therefore, that tool could not be reasonably relied upon for later use against that same or even another adversary. Once vulnerabilities are made public, they are patched by operating systems vendors and antivirus companies. Consequently, the tens of thousands of hours required to develop some cyber weapons could be wasted by frivolous use by a partner. Worse yet, the opportunity to use a weapon against a crucial target could be lost by a partner’s early use of that same weapon. The logic above does not entirely apply to cyber espionage tools, which, by nature, sit undetected for extended periods of time in a target’s cyber infrastructure. Therefore, the risk of instant obsolescence, as described above, is not as severe for cyber espionage tools.

So, what are the benefits of sharing of cyber weapons? Perhaps the most significant is that, like traditional weapons, smaller states rarely have the vast human and physical capital, nor organizational structures and industrial base required to develop complex cyber weapons. Advanced fighter aircraft, for example, are produced by only a handful of countries, which then export some of the aircraft to their partners. By sharing its cyber weapons, a larger, more powerful country can enable its smaller allies to be armed with advanced tools that can be used effectively against mutual adversaries. Taking this idea a step further, by choosing to arm its smaller allies, the exporter can enjoy greater international legitimacy for its causes. If a coalition partner is not able or willing to contribute to the kinetic fight, but can overtly employ cyber weapons against a common adversary, then the coalition leader gains many of the same benefits. The importing partner may also possess some sort of niche kinetic capability that a cyber weapon can support. For example, if the Arab Persian Gulf states came under threat from a new Iranian ballistic missile site and the UAE had the capability to destroy it with a deep-strike F-16 mission, but needed a cyber weapon to take down the Iranian air defenses, the United States, with its extensive offensive cyber capabilities, could build and provide that tool. This fictional scenario illustrates how a cyber weapons sharing partnership can effectively support the achievement of mutual strategic objectives. There is also the matter of larger, more powerful states wanting to hold onto the capability to build powerful cyber weapons, in much the same way that a small number of states seek to maintain a monopoly over nuclear weapons production. The United States may not want its smaller partners developing such weapons, and so may enter into sharing agreements for the sake of non-proliferation.

Conclusions

Some conclusions may be drawn from the discussion above. There are clear circumstances under which it would be beneficial to a large, powerful state to export its cyber weapons to smaller, less powerful allies. However, numerous safeguards must be put into place. In order to prevent proliferation and misuse, the cyber weapons must have incorporated into their design a sort of digital “dual key” feature that requires the consent of the exporting partner for each use. They must only be provided as compiled applications so that the importing country cannot modify the source code to build their own weapons. Signatures from the importing state must be programmed into the weapons as well in order to prevent misattribution of any use of the weapon to the exporting state. Certainly, this will significantly diminish the value of that weapon, as it will have no covert use capability, which is a key advantage of cyber weapons. The exporting country should not provide copies of cyber weapons from its own active arsenal, but rather, should develop tailored weapons for the importer. This requirement is due to the unique nature of cyber weapons in that the vulnerabilities they exploit are likely to be quickly patched across many systems worldwide soon after the weapon’s first use. The United States and other major cyber powers should consider all of these circumstances carefully and incorporate them into a cyber weapons sharing policy. Judicious sharing of cyber weapons under the right conditions and with the right protections can have major benefits to a state’s national security.

97

Great analysis and use of examples. Supporting your arguments with some theoretical sources would have made them even stronger. An interesting direction for future research might be the transfer of cyber defense systems.

# Works Cited

"Boeing Wins $6.2 Billion Qatar Contract for 36 F-15s." *St. Louis Today* 22 December 2017.

Elbagir, Nima, et al. "Sold to an Ally, Lost to an Enemy." *Cable News Network* February 2019.

England, Andrew. "Foreign Meddling and West's Incompetence Fuel Libyan Chaos." *Financial Times* 8 January 2020.

Hedge, Zero. "Wikileaks Unveils ‘Vault 7’: “The Largest Ever Publication Of Confidential CIA Documents”; Another Snowden Emerges." *GlobalResearch* 7 March 2017.

Kaidanow, Tina S. *Subcommittee on Terrorism, Proliferation, and Trade Committee on Foreign Affairs, US House of Representatives* 15 June 2017.

McQuade, Mike. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired* 22 August 2018.

Mehta, Aaron. "Here’s how many foreign military sales the US State Department OK’d in FY19." *Defense News* 4 October 2019.

*Non-Recurring Costs and Waivers*. Fact Sheet. Arlington, Virginia: Defense Security Cooperation Agency, 2018. Online.

Rounds, Ray. "The Case against Arms Embargos, even for Saudi Arabia." *War on the Rocks* 16 April 2019.

Schanz, Marc V. "Allies in the Gulf." *Air Force Magazine* 24 February 2015.

Warren, MSgt Timothy. "Defense Language Institute Looking for a Few Amigos." *The Alamo Wing* July 1995: 7.