Comparing Cyber Weapons to Traditional Weapons Through the Lens of Business Strategy Frameworks

Nicola Bates - Supervised by Konstantinos Markantonakis
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

- Increase knowledge of the cyber weapons domain required for decision making
- Compare cyber attacks and kinetic attacks which would achieve a similar effect or objective
- Determine the strengths and benefits of cyber weapons as well as the limitations and challenges

Introduction

Advances in technology have changed the way nation states conduct offensive operations with cyber capabilities increasingly used. However, cyber weapons possess different characteristics, deployment and impact mechanism than traditional weapons.

In this work business strategy frameworks are utilised to provide an insightful way to consider differences. Specifically, PESTLE, Porters Five Forces and SWOT methodologies are used to analyse trends and find power dynamics in order to support decision making.

What is a cyber weapon?

A cyber weapon relies on the three things:

1. A vulnerability: A weakness or design flaw that can be manipulated to obtain access to a system
2. An exploit: Code written to cause a specific effect through taking advantage of a vulnerability
3. A propagation mechanism: The way in which the exploit is delivered to the target

Effects identified for code to be considered a cyber weapon for the purposes of this work:

1. Political effects to control the environment or dictate the narrative
2. Have physical effects which cause destabilisation and confusion showing power and intent
3. Have physical effects which causes permanent damage to equipment or humans.

Ten attacks considered in analysis

* Estonia 2007	* Stuxnet 2010	* F-35 IP Theft 2013	* SWIFT 2015/16	* US election 2016
* Georgia 2008	* Aramco 2012	* Sony Pictures 2014	* Ukraine 2015	*WannaCry 2017

PESTLE Analysis

PESTLE stands for Political, Economic, Social-cultural, Technological, Legal and Environmental. Using PESTLE ten cyberattack are compared with alternative ways of achieving the same effects – a low-level and a high-level intensity kinetic example. These are ranked based on which achieve the best and worst outcomes for the aggressor and assigned a score weighted by PESTLE category, as shown in table 1. If the attack is particularly impactful (or not) in a certain category these scores are raised (or lowered) to reflect this. Table 2 shows Stuxnet scoring where Political, Technological and Environmental categories have been raised. Final scores are an indicative measure of the greatest return on effort for the attacker, for the cost incurred. A higher score indicates the superior option.

	P	E	S	T	L	E
Best	6	6	6	4	6	2
Medium	3	3	3	2	3	1
Worst	0	0	0	0	0	0

Table 1: Default PESTLE scoring for best, medium, worst ratings

	P	E	S	T	L	E	Total
Cyber	8	0	6	0	6	4	24
Special ops.	0	6	0	3	3	2	14
Missile strike	4	3	3	6	0	0	16

Table 2: PESTLE scoring for Stuxnet example

Porters Five Forces Analysis

Porters analyses underlying market forces and helps identify the attractiveness of industries and markets. In this context the model is used to analyse the underlying market for cyber weapons approached from the point of view of the cyber weapons developer. To understand how the competitive dynamics differ three levels of cyber weapon sophistication have been considered as shown in table 2.

	High complexity	Medium complexity	Low complexity
Attack examples	Stuxnet, WannaCry	Sony Pictures, Aramco, Ukraine, SWIFT, F-35 IP theft	Estonia, Georgia, US elections
Threat substitute products	No substitutable products available	Moderate substitutability, but options still complex to deploy	Products can be substituted to alternative tools and/or models
Threat protection vs attack	Threat of protection versus attack high. Utilisation will lead to protection	Medium risk of protection versus attack developing	Low to no threat protection. Method used repeatedly with immunity hard
Power buyers / suppliers	Overall balance: suppliers but buyer strong if government	Overall balance: suppliers	Overall balance: buyers
Rationality of market	Borderline irrational – opaque area prevents full arms race	Borderline rational – driven in part by fear of escalation	Cyber element rational Human element irrational

Table 3: Summary of Porters Five Forces analysis

Properties of cyber weapons

- Attribution: Difficult and usually probabilistic
- Proliferation: Reverse engineering allows reuse with spread cheaper and easier
- Diversity of actors: Private companies own much of the infrastructure. Individuals can have impact
- Speed: Almost instantaneous after groundwork
- Reach: Anywhere there are IT networks
- Dynamism: Domain can be changed at will
- Cost: Low end capabilities cheap but research and development expensive at high end capability
- Target dependance: High in complex weapons
- Under theorization: Strategic knowledge gap
- Threat assessment: Harder to complete
- Life expectancy: Lower than traditional weapons
- Intrusion and attack may look the same
- Improved defences counter attacks globally

Conclusion

PESTLE and Porters work allow completion of a SWOT analysis, to determine the Strengths, Weaknesses, Opportunities and Threats of cyber weapons.

Cyber weapons are attractive due to their:

1. Deniability
2. Action at a distance with close quarters accuracy
3. Rapid strike without warning across entire networks
4. Ability to have limited and reversible effect
5. Effectiveness when augmented with kinetic ability
6. Enabling faster and cheaper influence operations

Cyber weapons give challenges in their:

1. Fragile indiscriminate destructive capability
2. Becoming effectively open source once launched, giving containment and proliferation issues
3. Groundwork being time consuming
4. Requiring scarce/expensive experienced personnel

Contact

nicola.bates.2018@live.rhul.ac.uk