INSS Insight No. 444, July 8, 2013

The Use of Code Mutation to Produce Multi-use Cyber Weapons

Daniel Cohen and Aviv Rotbart

The increasing use of cyber weapons is creating the inevitable situation in which sophisticated versions of cyber weapons capable of generating strategic damage will fall into the hands of states that support terrorism, terrorist organizations, and criminal organizations. Cyber weapons will no longer be the exclusive province of the few. The Stuxnet virus attack on the Iranian nuclear facilities is one such example. For years it operated undetected, but the moment it was discovered the virus code was subjected to in-depth analysis. The results of this research can immediately be put to use to develop new viruses operating similarly to the Stuxnet virus. In other words, once a secret is out, weapons spread.

In biology, the term genetic mutation is used to describe an error in DNA reproduction. Mutations cause differences between organisms; thanks to mutations, organisms can adapt to the environment. When a virus mutates, the virus has had its genes altered in some way, and this change affects some of its features, perhaps making it more resistant to the human immune system, or deadlier, or able to spread more easily. Every flu season there are new mutations in familiar viruses.

A common misconception about cyberspace is that once a computer virus or other malware used in an attack is discovered by the security companies, it is rendered useless for future use, because the anti-virus software has identified it and developed immunity against it, depriving it of its ability to cause damage. In other words, computer viruses are disposables, meant for one-time use. But this is not the case. Similar to biological viruses, malicious code can also evolve, making it more resistant to anti-virus software. This kind of code is known as code mutation. Its uniqueness lies in the fact that although it has similar functional features to the parent code from which it was created (to the point of being identical), the difference is syntactic (structural) rather than semantic, in order to elude the radar of software detecting malware.

How is code mutation created? Similar to a genetic mutation, the mutant code does not have to differ greatly from the original code. Computer code, including virus code, usually consists of several software components that communicate in order to carry out

tasks. Sometimes, a small change in the way the components communicate with one another or in one of the components itself is enough to create a code mutation undetectable by the computer's immune system – the security and anti-virus software. At times more significant changes are necessary, processes that will cause the malicious code to look very different than the original code that was the basis for its creation. But these changes are for the sake of appearance only. After the virus passes the computer's firewalls and other defensive measures, it reverts to its original form and starts to function like the original virus. Two known methods to alter computer code are called, in the world of computer software, obfuscation and packing. These will change the code (make it look like a picture, text, or a string of meaningless keystrokes) but will not impact its functionality.

The strategic environment of the cyber battlefield includes the use of cyber weapons to penetrate the enemy's systems for espionage, psychological warfare, deterrence, or damage to telecommunications or physical systems. Cyberspace offers wide-ranging warfare opportunities for many players who can operate in it according to their specific interests using their particular capabilities. The weapons arsenal includes advanced capabilities, usually found in just a few countries, and includes the ability to penetrate enemy systems without detection, gather intelligence, disrupt activity without arousing suspicion, and even cause physical damage to systems connected to cyberspace. The arsenal also includes simpler, less expensive weapons – used by other players such as criminal organizations, terrorist organizations, and commercial institutions – that are generally used to achieve temporary network damage (denial of service attacks), penetrate computer networks lacking a high level of security, steal information, and cause disruption. Capabilities such as these are for sale on the internet, increasing the proliferation of cyber weapons and making them accessible also for those lacking technological capabilities but equipped with the money to buy them.

The ability to create code mutation has reduced the technological gap between cyberspace actors. While state capabilities are required to create a sophisticated cyber weapon, all that is needed to duplicate it or create mutations is a group of talented civilian hackers that can use it to their own ends or sell it and operate it for others in exchange for payment.

At present, the internet and other communications networks based on similar protocols are insufficiently secured against a motivated attacker. The state's dependence on the internet and the reliance of a variety of sectors on cyberspace make the cyber realm highly attractive, both to terrorist organizations seeking to penetrate the public's consciousness and change an existing political reality, and to criminal organizations interested in financial profit. Both can achieve their goals through an attack in

cyberspace, which is often cheaper and simpler than kinetic terrorism and crime but capable of attaining a similar effect.

The features of the cyber battlefield place the attacker before dilemmas stemming from the fact that cyber weapons are multi-use weapons. Their use informs the victim of their characteristics, allowing the victim to use them as well, even as a retaliatory measure against the attacker (the boomerang effect). Weapons with strategic destruction capabilities (such as Stuxnet) are liable to fall (or have already fallen) into the hands of states supporting terrorist and criminal organizations and provide them with a basis for cyber attacks.

The decreasing costs and increasing availability of cyber weapons to terrorist and criminal organizations are a threat to state security in general, and the State of Israel in particular. As states make increasing use of cyber weaponry, their proliferation at the hands of other nations and non-state entities is to be expected. Therefore, when analyzing cyber threats, cyber weapons must be regarded as multi-use weapons that can be exploited for future attacks.