

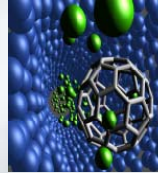
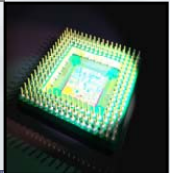
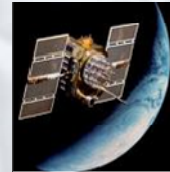
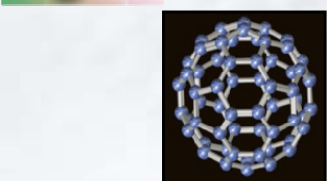
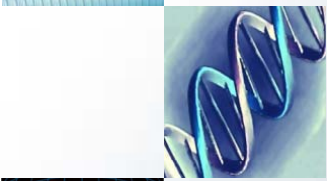
Cyber Weapons

Threat Matrix
From

SpyOps

technolytics

INTELOMICS
SUPERIOR INTELLIGENCE THROUGH TECHNOLOGY



With 120 countries now in the cyber arms race, intelligence agencies around the world are working to assess their offensive and defensive cyber capabilities. Developing cyber weapons does not require the massive infrastructure usually associated with conventional arms. A couple of PCs and a couple of smart programmers and you have all you need to create a cyber weapon. Advanced Cyber Weapons have unique capabilities that make their detection and elimination much more difficult than conventional viruses and Trojans of years gone by. As with the conventional arms race, countries with significant defense spending have taken the lead in the cyber arms race. But that trend is rapidly changing. In the past few years malicious code with advanced features has been created for under \$3,500 USD. We are beginning to see the emergence of cyber arms dealers. The cost of cyber weapons are in range of poor and developing countries. For these reasons the Technolytics Institute in conjunction with Intelomics and Spy-Ops have worked together and create the following Cyber Weapons Threat Matrix.

Cyber Weapons Threat Matrix

Threat	Threat Color Code	Working Definition	2004 Threat Rating	2006 Threat Rating	2008 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Logic Bomb	3.7	A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as the salary database), should they ever leave the company.	3.5	3.8	4.1	3.7	4.0	3.2
Computer Virus	3.8	Malicious software that attaches itself to other software. For example, a patched software application in which the patch's algorithm is designed to implement the same patch on other applications, thereby replicating itself.	3.5	3.8	4.1	3.0	4.0	4.5
Rabbit	2.8	This is a form of computer virus or worm that replicates without bound, thus exhausting available computing resources, but it does not spread to other systems.	3.0	3.1	3.1	2.5	3.0	2.3
Bacterium	3.0	A form of computer virus designed to attach itself to the OS in particular (rather than any application in general) and exhaust computer resources, especially CPU cycles.	3.0	3.3	3.9	2.5	3.0	2.3

Cyber Weapons Threat Matrix

Threat	Threat Color Code	Working Definition	2004 Threat Rating	2006 Threat Rating	2008 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Spoofing	3.0	In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.	3.3	3.5	3.8	3.0	2.4	2.0
Sequential Scanning	3.5	In the sequential scan, worms in an infected host will select randomly an IP address in an effort to identify system vulnerabilities.	3.1	3.5	4.1	3.2	3.2	3.7
Dictionary Scanning	3.4	This type of attack exploits a buffer overflow vulnerability in targeted client software through injection of malicious content from a custom-built hostile service.	2.9	3.4	4.0	3.2	3.5	3.6
Digital Snooping	3.3	This is the electronic monitoring of digital networks to uncover passwords or other data. It has grown with the rapid adoption of wireless lans.	1.8	2.6	4.0	3.8	3.8	3.7
Spamming (DoS, DDoS)	2.9	This is the intentional overloading a system with incoming messages or other traffic to cause system crashes.	1.9	2.9	4.1	1.0	4.1	3.5
Tunneling	3.5	This refers to any digital attack that attempts to get "under" a security system by accessing very low level system functions (e.g., device drivers, OS kernels).	2.9	3.4	3.9	3.2	3.5	3.8

Cyber Weapons Threat Matrix

Threat	Threat Color Code	Working Definition	2004 Threat Rating	2006 Threat Rating	2008 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Scavenging	3.3	This is associated with automated scanning of large quantities of unprotected data (discarded media or online "finger" type commands) to obtain clues as to how to achieve access.	2.9	3.3	3.6	3.2	3.5	3.2
Counterfeit Equipment	3.6	Counterfeit hardware refers to an imitation that is made usually with the intent to deceptively represent its content or origins and with unknown integrity.	3.0	3.7	4.2	4.9	3.5	2.5
Counterfeit Software	3.6	Counterfeit software refers to an imitation that is made usually with the intent to deceptively represent its content or origins and with unknown integrity.	3.0	3.7	4.2	4.9	3.5	2.5
Software Malfunction	3.9	This refers to software behavior that is in conflict with intended function or operation that pose a security risk.	3.0	3.7	4.2	4.0	4.0	4.6
BotNets	3.0	BotNet is a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software, but it can also refer to the network of computers using distributed computing software.	2.5	3.0	4.5	1.0	4.0	3.0

Cyber Weapons Threat Matrix

Threat	Threat Color Code	Working Definition	2004 Threat Rating	2006 Threat Rating	2008 Threat Rating	Detection Difficulty	Current Availability	Current Usage
Trap Door / Back Door	3.5	Software left available after code delivery for the purpose of future access.	3.0	3.2	3.5	4.5	3.0	3.5
TEDs/EPFCs/EMP (non-Nuclear)	3.0	These devices generate electromagnetic radiation from an explosion or an intensely fluctuating magnetic field caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the electronic or explosive device or in a surrounding medium.	2.2	3.5	3.8	3.8	3.2	1.5
Insider Threat	3.7	An insider threat is an individual with malicious intent. Typically it is someone who is an employee or officer of a business, institution, or agency. The term can also apply to an outside person who poses as an employee or officer by obtaining false credentials.	3.0	3.5	3.8	4.0	3.5	4.3
Trojan Horse	3.7	A Trojan horse, also known as a trojan, is malware that appears to perform a desirable function but in fact performs undisclosed malicious functions. Therefore, a computer worm or virus may be a Trojan horse.	3.0	3.5	3.8	3.5	4.0	4.3

About Technolytics

technolytics

The Technolytics Institute (Technolytics) was established in 2000 as an independent executive think tank. Our primary purpose is to undertake original research and develop substantive points of view on strategic issues facing executives in businesses and industry around the world. Our strategic goals focus on improving business performance, creating sustainable competitive advantage, delivering innovation and technology, and managing security and risk.

Technolytics help guide business executives, industry leaders and government policy makers in shaping the economic, regulatory and risk environment of tomorrow. One of the Hallmarks of our service offering is our security and risk scenario planning. Our approach is called Trans-disciplinary Intelligence Engineering (TIE). This approach has been used to develop scenarios for Homeland Security, Corporate Event Planning, Corporate Espionage and Security and for other entities. This technique has been applied to strategic planning, product strategy, competitive strategy and marketing strategy as well as security and risk management.

Our technology framework methodology is based upon 1997 Malcolm Baldrige strategic planning and reporting guidelines. We believe these guidelines (as implemented in the Technolytics models and tools) represent some of the best strategy and management models available anywhere in the world. The knowledge repository, benchmark data, and best practices used to create these Technolytics models have evolved from detailed research and analysis and are updated regularly to reflect changes in the global market.

The Technolytics Institute
4017 Washington Road
Mail Stop #348
McMurray, PA 15317
P 412-818-7656
F 412-291-1193
I www.technolytics.com
E kgcolman@technolytics.com