

Cyber Threat Landscape for the Medical Community

G. Alexander Crowther, Ph.D.

Jack D. Gordon Center

Florida International University

alex.crowther@ndu.edu

Types of Cyber Operations

Cyber Operations	Any action taken in cyberspace
Information Operation	Cognition shaping, much of which happens in cyberspace
Intelligence Operation	Gathering important information and analyzing it; much information gathering happens in cyberspace
Cyber crime	Crime that occurs in cyberspace. Important and growing number of cyber operations
Cyber attack	An armed attack in cyberspace. Usually requires one of these results: <ul style="list-style-type: none">• Property damaged• Property destroyed• Person hurt• Person killed

Cyberspace Operation Sequence

Before Initial Entry	Preparation of malware Selection of target (Social Engineering)
Initial Entry	Phishing operation Placing hardware into the system
Reconnaissance	Exploring the network Identifying Administrators & Leaders Assessing vulnerabilities
Preparation to create effect	Putting in Backdoor Changing software to allow you to create your chosen effect
Creation of effect	Moving money Taking information Denial of Service

Cyber Breaches 2019

- April 2019 saw a “not completely disastrous” 1,334,488,724 breached records. That’s better than last month, bringing the annual total to 5.64 billion and reducing the monthly average to 1.46 billion
- 27 of 74 breaches involved Medical organizations
- Cyber Infiltration
 - California, Florida, Idaho, Illinois, Massachusetts, Minnesota, South Carolina, Texas (x3)
- Ransomware
 - Massachusetts, New Jersey, Pennsylvania
- Data breaches
 - Canada, India, Russia
 - Ohio (x3), Pennsylvania, Puerto Rico, Texas, Washington State
- Malicious insiders and miscellaneous incidents
 - California, Maine, Ohio (x2)

Typical Cyber Operations

	Patient Information	Research	Money	Ransom
States		X	X	
Proxies	X	X	X	X
Terrorists	X		X	
Hacktivists	X	X	X	X
Business	X	X		
Criminals	X	X	X	X

What are they coming for?

- Research
 - Predilection for disease
 - Intelligence
 - Politics
 - Insurance
 - Biologics
 - Market your research
 - Create a specific toxin
- Money
 - Steal money electronically
 - Ransom
 - Denial of service
 - Ransomware

Operators and Operations

Operators & Target Audiences:

- States
- International Organization
- Proxies
- Terrorists
- Hacktivists
- Business
- Criminals
- The Population
- The Co-opted

Types of Operations:

- Shaping Cognition
- Intelligence
- Crime
- Cyberspace Attacks

Most Probable Cyber Operations

		Targets								
		States	Intl Orgs	Proxies	Terrorists	Hacktivists	Business	Criminals	Populations	Co-Opted
Actors	States	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Attack	Info Intel Crime Attack	Info Intel Attack	Info Intel Attack	Info Intel Attack	Info Intel Attack	Info Intel Attack (through)
	Proxies	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Attack	Info Intel Crime Attack	Info Intel Crime Attack
	Terrorists	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Attack	Info Intel Crime Attack	Info Intel Attack	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Crime Attack	Info Intel Crime Attack
	Hacktivists	Info Intel Attack	Info Intel Crime Attack	Info Intel Attack	Info Intel Attack	Info Intel Attack	Info Intel Attack	N/A	Info	Info Intel Attack
	Business	Info Intel	N/A	Info Intel	Intel Attack?	Intel	Intel Crime	Intel Attack?	Info Intel	N/A
	Criminals	Info Intel Crime	Info Intel Crime	Info Intel Crime	Info Intel Crime	Info Intel Crime	Info Intel Crime	Info Intel Crime Attack	Info Intel Crime	Info Intel Crime
	Populations	Info Intel	N/A	N/A	N/A	N/A	N/A	Info Intel	Info Intel	N/A

Most Probable Cyber Operations Against You

		Medical Businesses
Actors	States	Info Intel Attack
	Proxies	Info Intel Crime Attack
	Terrorists	Info Intel Crime Attack
	Hacktivists	Info Intel Attack
	Business	Intel Crime
	Criminals	Info Intel Crime
	Populations	N/A

Medical Cyber Operations

Most Likely

Least Likely

Worst Case

Ransom

Genetically-
designed Toxins

Best Case

Positive Impact
on Research

Major medical
breakthrough

	Most Likely	Least Likely
Worst Case	Ransom	Genetically- designed Toxins
Best Case	Positive Impact on Research	Major medical breakthrough

Computer Fraud & Abuse Act (CFAA)

- Enacted in 1986
- Amendment to existing computer fraud law ([18 U.S.C. § 1030](#)),
- Caused by 1983 techno-thriller film WarGames
- Amended a number of times—in 1989, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act.
- Generally prohibits intentionally accessing a computer, without authorization (or exceeding authorized access), and obtaining information from a protected computer.

Cyber Training & Education

Senior Leaders	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your profession	How to supervise the use of technology	How to prioritize and resource Cybersecurity and Education in your organization
Supervisors	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your profession	How to supervise the use of technology	
Students of Professions (e.g. Medical School)	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your profession	How to supervise the use of technology	
Workers	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your work		
College Students	Cyber Hygiene	Responsible use of Information and Information Technology	Productive use of technology		
High School Students	Cyber Hygiene	Responsible use of Information and Information Technology			
K-8/Every Citizen	Cyber Hygiene				

Cyber Training & Education

Senior Leaders	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your profession	How to supervise the use of technology	How to prioritize and resource Cybersecurity and Education in your organization
Supervisors	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your profession	How to supervise the use of technology	
Students of Professions (e.g. Medical School)	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your profession	How to supervise the use of technology	
Workers	Cyber Hygiene	Responsible use of Information and Information Technology	Use of technology in your work		