Cyber Warfare Demystified

Imagine building a fortress,
but instead of stone and mortar, it's made of computer programs.

That's how our world works now !

with crucial systems like power grids and communication networks relying on software. While we try our best to build these programs perfectly, just like any wall, they can have weak spots - called vulnerabilities.

Some countries, like Russia, China, and the US, see exploiting these weak spots in other countries' programs as a new battleground, called "**Cyber Warfare**."

It's like using secret codes to sneak into the fortress and mess things up. They might do this to steal information, spread rumors, or even cause disruptions.

This might sound scary, but there's good news! Just like we can improve our physical fortresses, we can learn how to protect our digital ones. **By understanding these vulnerabilities and being responsible online**, we can all play a part in keeping our "software fortresses" strong.

"Cyber warfare is not a future possibility, but a present reality. It is not a hypothetical scenario, but a daily occurrence. It is not a distant threat, but an imminent danger." *Leon Panetta*

Definition: Cyber Warfare (CW) refers to the strategic use of cyber tools and techniques by state or non-state actors to achieve specific objectives, often with the intent to cause harm or disruption to critical infrastructure, systems, or individuals, potentially impacting national security, economy, or society.

Tools

1. Information Gathering: These tools gather information, but their impact can be significant. For example, stolen data can be used for blackmail or economic espionage. Remember, using these tools ethically and legally is crucial.

2. Malware: This malicious software can disrupt essential services like power grids or hospitals. New AI-powered malware variants pose an emerging threat.

3. Offensive Hacking: Hackers might exploit vulnerabilities to steal sensitive information or manipulate elections. These actions can have significant legal and ethical consequences.

4. Physical Intrusions: Gaining physical access to hardware can cause serious damage, highlighting the importance of physical security measures.

5. Social Engineering: Manipulating people can trick them into revealing sensitive information or clicking malicious links. Be aware of these tactics and practice cyber hygiene.

Let's delve into the three main categories that define the "**why**" behind cyberattacks:

1. Information Intelligence: Piercing the Veil of Secrecy

Imagine piecing together a puzzle from diverse sources: radio signals, satellite imagery, open-source data. ASI operates in this enigmatic fashion, employing Artificial Intelligence to harness a vast array of sensors and glean critical insights into adversaries. Targeting enemy communications, data centers, and even radiowaves, ASI aims to create an all-encompassing situational awareness, empowering strategic decision-making. By harnessing disciplines like CYBINT (cyber intelligence), SIGINT (signals intelligence), and OSINT (open-source intelligence), ASI becomes a formidable tool for intelligence gathering while maintaining covert operations.

2. Information Confrontation: Weaponizing Narratives and Perceptions

The battlefield expands beyond physical borders in the age of information. Here, the struggle for control over narratives and perceptions takes center stage. Information confrontation tactics aim to manipulate public opinion, disrupt decision-making processes, and ultimately, gain an advantage over opponents. This can involve disinformation campaigns, where fabricated narratives and content are strategically disseminated to mislead audiences. Additionally, denial of information tactics aim to restrict access to accurate information during critical moments, further obfuscating the truth and hindering informed decision-making. This category highlights the growing importance of critical thinking and media literacy in today's information-saturated world.

3**. Disruption & Loss: Crippling Infrastructure, Causing Mayhem**

Not all cyberattacks target data; some aim to cause tangible harm. This category encompasses attacks on critical infrastructure like power grids, transportation networks, and even nuclear facilities. The goal is to inflict economic damage, disrupt essential services, and create widespread chaos. The rise of ransomware and wiper malware exemplifies this approach, encrypting or destroying vital data to cripple victims and extract concessions. This category serves as a stark reminder of the potential societal impact of cyberattacks, necessitating robust cybersecurity measures and international cooperation to mitigate these risks.

Cyber warfare is not a game of chess, but a game of go. The objective is not to capture the king, but to surround the territory.

Sara Malik <smk@PakCrypt.Org> is an InfoSec professional in PakCrypt outreach program.