Information Warfare

Lecture 3

What is Information Warfare

Information warfare refers to the use of information and communication technologies to gain a strategic advantage in military, political, or economic conflicts. It involves the deliberate manipulation, exploitation, or disruption of information systems and communication networks to achieve specific objectives.

Information Warfare Strategy

Defensive and **Offensive information warfare** are two distinct strategies of cyber operations and information security

Defensive		Offensive
1.	Cybersecurity Practices	Cyber Espionage
2.	Incident Response	Cyber Attacks
3.	Encryption	Denial of Service (DoS) Attack
4.	Access Control	Advanced Persistent Threats (APTs)
5.	Security Awareness Training	Disinformation and Propaganda
7.	Vulnerability Management	Data Manipulation
8.	Security Monitoring and Analytics	Hardware Tampering

Information Warfare Strategy

Defensive and **Offensive information warfare** are two distinct strategies of cyber operations and information security

Defensive information warfare focuses on protecting one's own digital assets, networks, and information from cyber threats and attacks. The primary goal of defensive information warfare is to ensure the confidentiality, integrity, and availability of data and systems while safeguarding against unauthorized access, data breaches, and other cyber incidents

Defensive information Warfare

1. **Cybersecurity Practices**: Implementing robust cybersecurity practices, including firewalls, intrusion detection systems, antivirus software, and regular security updates to defend against common cyber threats.

2. **Incident Response:** Developing and practicing incident response plans to swiftly detect, contain, and mitigate cyber incidents when they occur.

3. **Encryption:** Using strong encryption methods to protect sensitive data, ensuring that even if it's intercepted, it remains unintelligible to unauthorized parties.

4. **Access Control:** Managing user access to networks and systems through authentication mechanisms, least privilege principles, and multi-factor authentication.

Defensive information Warfare

5. Security Awareness Training: Educating employees and users about cybersecurity best practices, recognizing phishing attempts, and being vigilant about potential threats.

6. Vulnerability Management: Regularly scanning and patching systems for known vulnerabilities to prevent exploitation by malicious actors.

7. Security Monitoring and Analytics: Continuously monitoring network and system activity for signs of potential security breaches or anomalous behavior.

Offensive information Warfare

Offensive information warfare involves taking proactive actions to target and exploit the digital assets and infrastructure of adversaries. The primary objective is to gain a strategic advantage, disrupt the adversary's operations, or extract sensitive information

1. **Cyber Espionage:** Using sophisticated hacking techniques to infiltrate an adversary's networks and steal sensitive or classified information.

2. **Cyber Attacks:** Launching targeted cyber attacks to disrupt or disable an adversary's critical infrastructure, communication systems, or other vital services.

3. **Denial of Service (DoS) Attacks:** Flooding an adversary's systems or networks with excessive traffic, causing them to become unresponsive or unavailable.

Offensive information Warfare

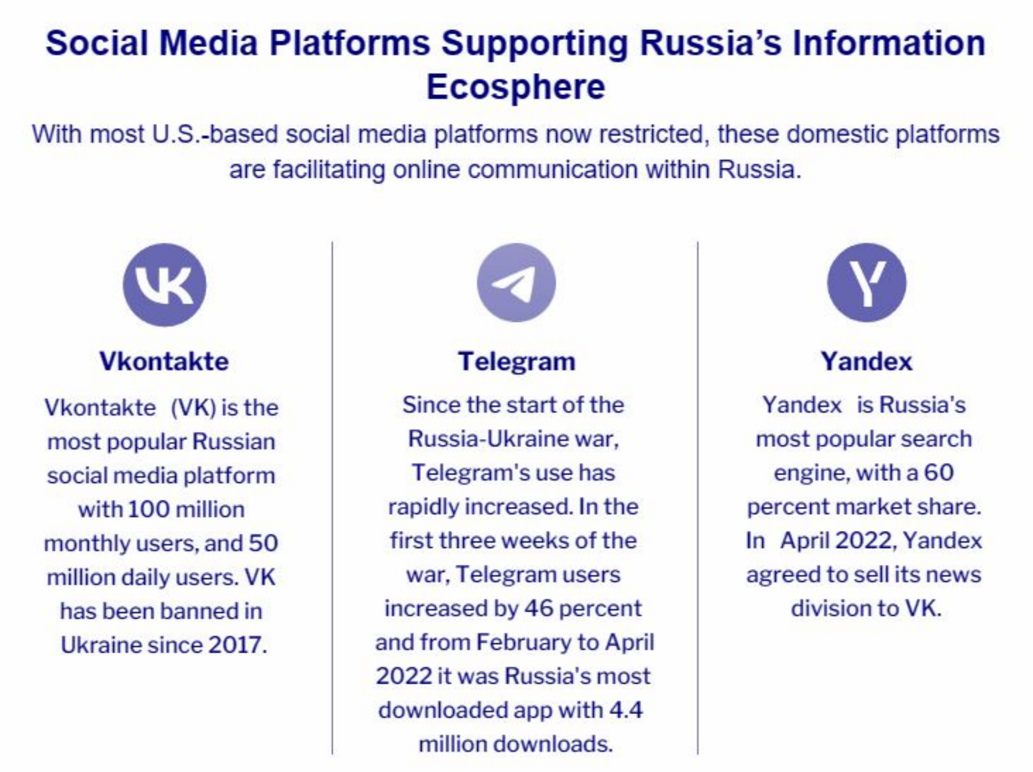
4. Advanced Persistent Threats (APTs): Employing long-term and stealthy cyber campaigns to gain access to an adversary's systems and remain undetected for extended periods.

5. Disinformation and Propaganda: Using social media and online platforms to spread false or misleading information, influencing public opinion or sowing discord.

6. Data Manipulation: Tampering with or altering data in an adversary's systems to undermine their operations or decision-making processes.

7. Hardware Tampering: Mass tampering any computer hardware in production level to surveillance other state or country.

Information Warfare - Russia Ukraine



Social Media Platforms Supporting Russia's Information Ecosphere

With most U.S.-based social media platforms now restricted, these domestic platforms are facilitating online communication within Russia.

Vkontakte

Vkontakte (VK) is the most popular Russian social media platform with 100 million monthly users, and 50 million daily users. VK has been banned in Ukraine since 2017.

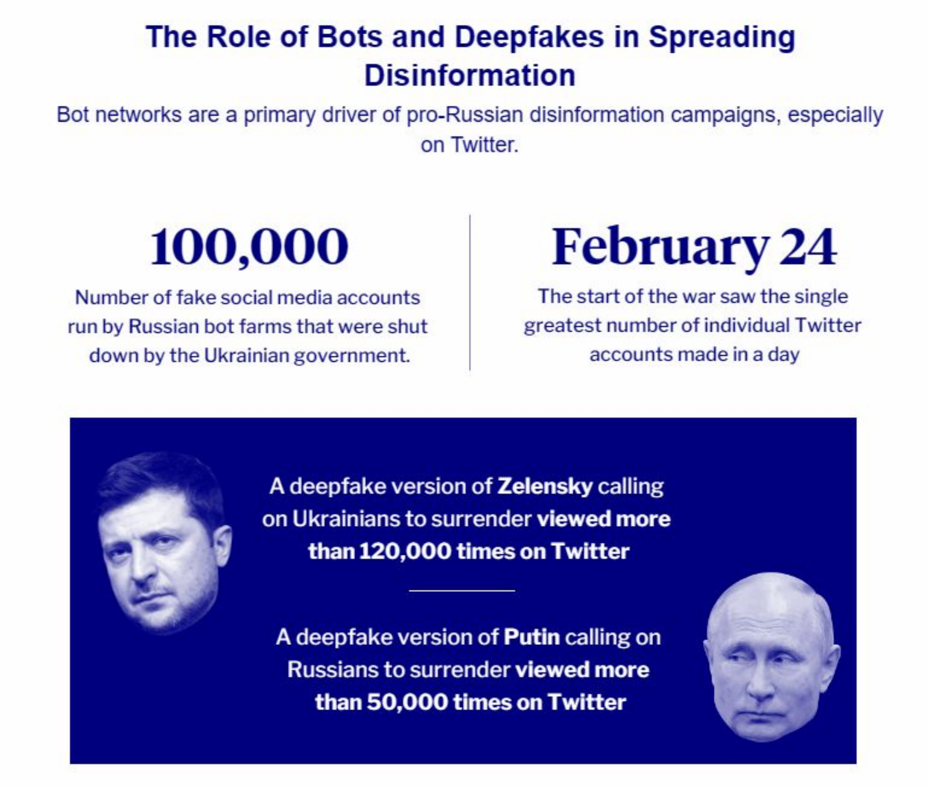
Telegram

Since the start of the Russia-Ukraine war, Telegram's use has rapidly increased. In the first three weeks of the war, Telegram users increased by 46 percent and from February to April 2022 it was Russia's most downloaded app with 4.4 million downloads.

Yandex

Yandex is Russia's most popular search engine, with a 60 percent market share. In April 2022, Yandex agreed to sell its news division to VK.

Information Warfare - Russia Ukraine (Cont.)



The Role of Bots and Deepfakes in Spreading Disinformation

Bot networks are a primary driver of pro-Russian disinformation campaigns, especially on Twitter.

100,000

Number of fake social media accounts run by Russian bot farms that were shut down by the Ukrainian government.

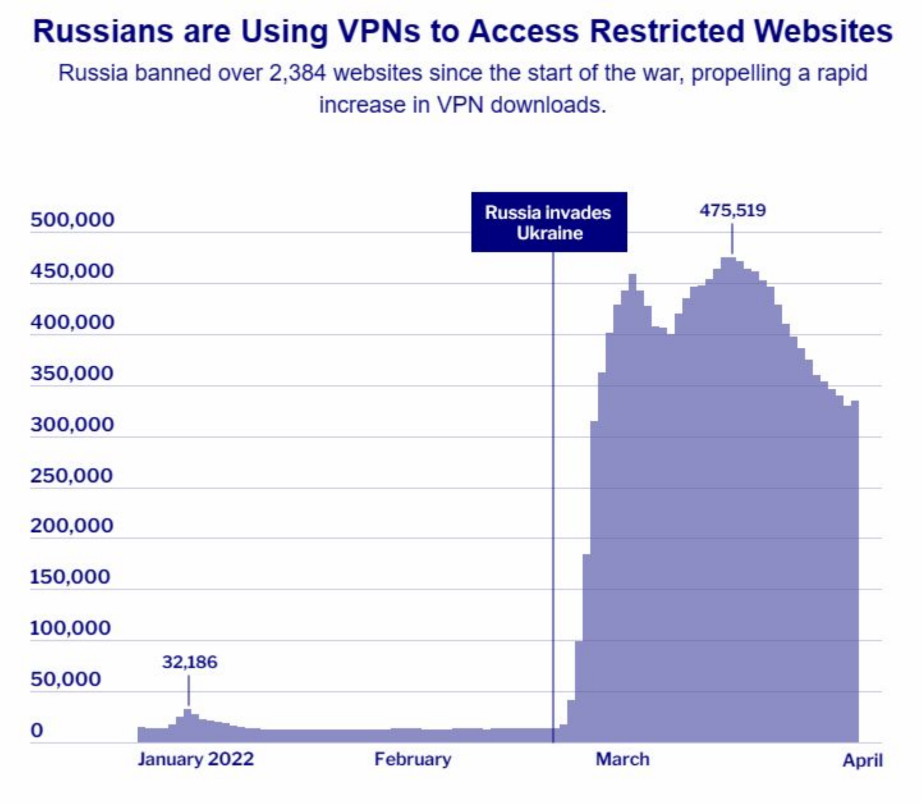
February 24

The start of the war saw the single greatest number of individual Twitter accounts made in a day

A deepfake version of **Zelensky** calling on Ukrainians to surrender **viewed more than 120,000 times on Twitter**

A deepfake version of **Putin** calling on Russians to surrender **viewed more than 50,000 times on Twitter**

Information Warfare - Russia Ukraine (Cont.)



Russians are Using VPNs to Access Restricted Websites

Russia banned over 2,384 websites since the start of the war, propelling a rapid increase in VPN downloads.

Use Of Deepfake In Information Warfare

Questions

Thanks!