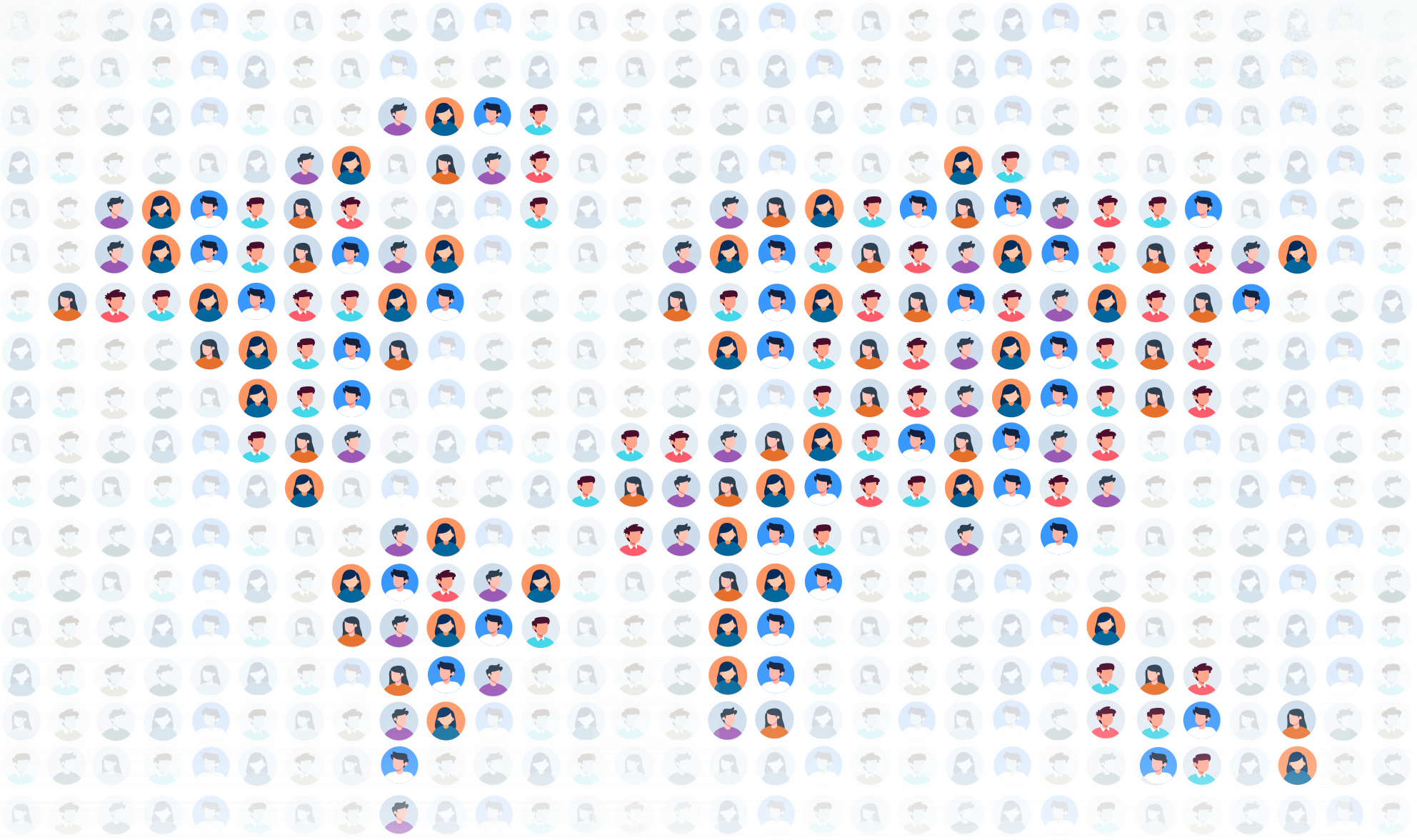


THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

مهارات
Maharat

THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

This manual was prepared by Maharat Foundation, with the support of UN Women and the French Embassy in Beirut.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

MODULE 1

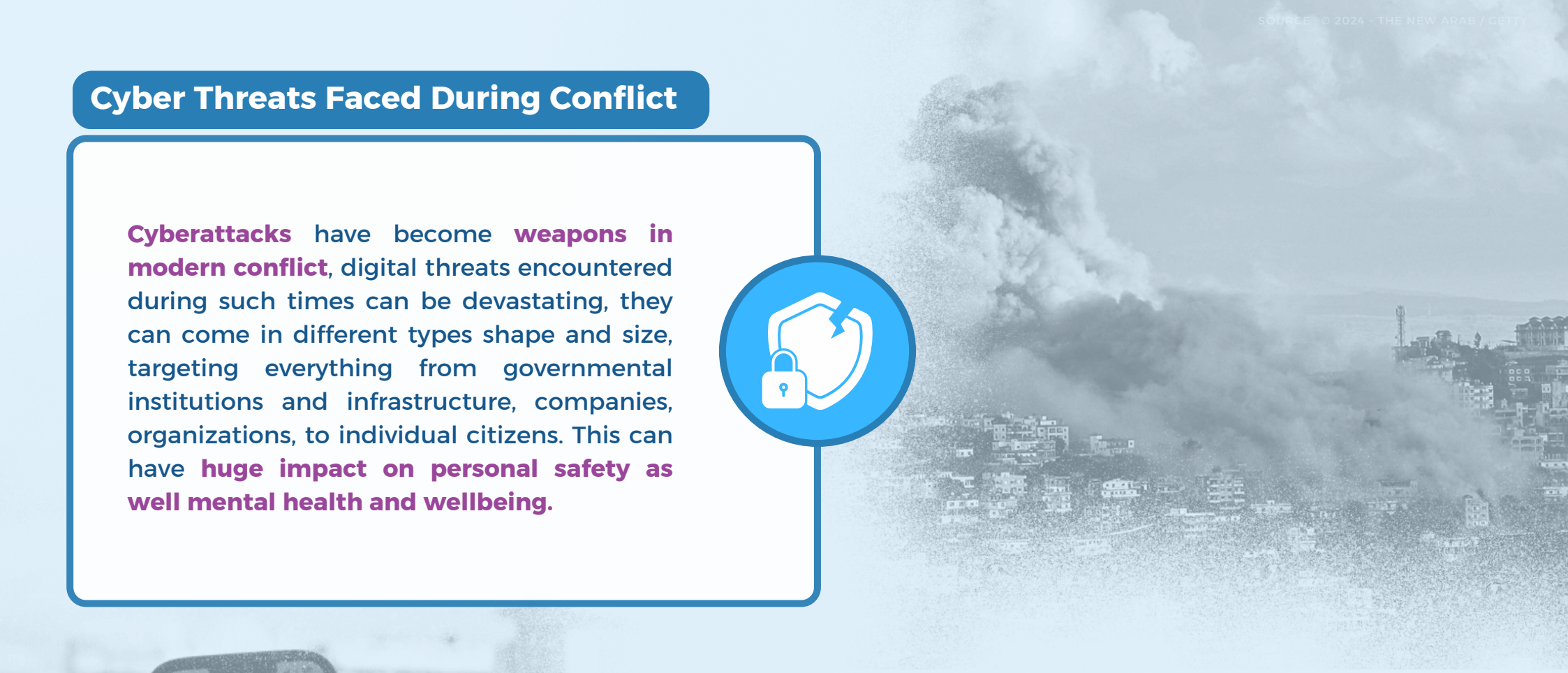
UNDERSTANDING DIGITAL THREATS:

Overview of common cyber threats faced during **conflict** (hacking, phishing, surveillance).

Prepared by:
Digital security expert
Bahaa Nasr

Cyber Threats Faced During Conflict

Cyberattacks have become **weapons in modern conflict**, digital threats encountered during such times can be devastating, they can come in different types shape and size, targeting everything from governmental institutions and infrastructure, companies, organizations, to individual citizens. This can have **huge impact on personal safety as well mental health and wellbeing.**



SOURCE : © 2024 - THE NEW ARAB / GETTY

SOURCE : © 2024 - JOSEPH EID/AFP

The most common cyber threats are **hacking, phishing, and surveillance.** These tactics can be used by state-sponsored actors, organized cybercriminal groups, or individuals with malicious intent. Each threat has its distinct features, but all aim to exploit weaknesses in digital systems and human behavior.

1 Hacking: Breaching the Digital Frontlines

Hacking is one of the most widely recognized cyber threats. In the context of cyberwarfare, hacking involves **unauthorized access** to computer systems or networks, often to steal, manipulate, or destroy data. **The goals** behind hacking operations can vary greatly, ranging from **espionage and sabotage to financial gain or psychological warfare.**

Data Breaches:

Hackers may target databases containing sensitive information, such as personal data (Names, addresses, phone numbers...), military plans, or government strategies. By gaining access to such databases, attackers can target specific target groups, blackmail individuals, or sell the data to hostile entities, leak information... Such attacks can cause widespread panic.

Defacement:

Website defacement involves hackers **taking control** of a website and altering its appearance or content, often to **disseminate propaganda or misinformation**. This tactic is used to undermine confidence in a government or organization, confusion, or mock the opposition.

Denial-of-Service (DoS) Attacks:

These attacks flood a network or website with excessive traffic, overwhelming its resources and rendering it inaccessible to users.

Ransomware Attacks:

Ransomware involves encrypting a victim's files and demanding payment (usually in cryptocurrency) for the decryption key. Ransomware can target both public and private sectors, paralyzing essential services such as hospitals, and communication networks.

The impact of hacking in conflict can be devastating.

A well-coordinated hacking campaign can bring an entire economy to a standstill, spread fear among the population, and weaken a nation's ability to respond effectively to the physical conflict.

2 Phishing: Exploiting Human Vulnerability

Phishing is a form of cyberattack that leverages social engineering to **deceive individuals into revealing sensitive information.** Phishing attacks can be sophisticated, they might try to take advantage of the heightened stress, confusion, and fear that accompany crises. Phishing focuses on **manipulating human behavior to achieve its objectives.**

How Phishing Works

Phishing attacks typically involve **sending fraudulent emails, messages, or websites that appear legitimate** but are designed to trick users into providing personal information such as login credentials, financial details, or other sensitive data.

Attackers often **impersonate trusted institutions**, such as banks, social media companies, government agencies, or employers, to increase the likelihood of success.

Spear Phishing: is a highly targeted form of phishing where **attackers tailor their messages to specific individuals or organizations.** Spear phishing campaigns are common during conflicts, as **attackers may target political figures, journalists, or military personnel to gain access to critical information.** For instance, state-sponsored actors may craft emails that mimic official government communication, luring targets into sharing classified data.

Phishing attacks usually exploit the **chaos and uncertainty of the situation during the war.**

EXAMPLE

For example, attackers may pose as **humanitarian organizations asking for donations** or as government agencies providing urgent safety information.

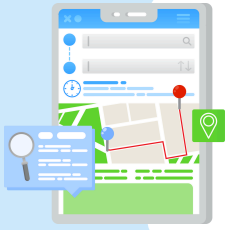
These messages often carry malicious attachments or direct users to fake websites designed to harvest login credentials or install malware on their devices.

3 Surveillance: Watching and Controlling the Digital Battlefield

Surveillance is another critical digital threat, particularly when it comes to **tracking, monitoring, and controlling the communication and activities of individuals or groups**. Surveillance technologies can be used by **governments, military forces, or hostile actors** to gain intelligence, control populations, and suppress opposition.

A Types of Surveillance

Electronic Surveillance: This involves monitoring communication channels such as emails, phone calls, and text messages. Hackers, governments or intelligence agencies may intercept communication to gather information about the movements, plans, or allegiances of individuals or groups involved in the conflict.



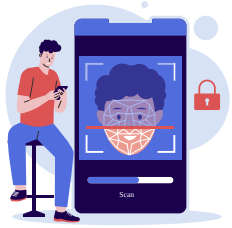
Location Tracking: Mobile devices, GPS systems, and social media can be used to track the physical location of individuals. In conflict zones, this can be used to monitor the movements of military personnel, political activists, or journalists. Location tracking can also facilitate targeted attacks, such as drone strikes or raids.

Mass Data Collection: Governments and organizations may collect vast amounts of data from citizens, such as internet usage, social media activity, or browsing habits. This data can be analyzed to identify dissidents, suppress opposition, or preemptively neutralize threats.

B Surveillance during war

In times of conflict, surveillance can be a **double-edged sword**. On the one hand, it can be used for **national security**, enabling governments to detect and respond to threats quickly. However, surveillance can also be used to **oppress dissent, violate privacy rights, and suppress freedom of speech.** In authoritarian regimes, surveillance tools are often employed to **crack down on protestors, activists, and journalists, leading to mass arrests and human rights violations.**

The rise of sophisticated surveillance tools, such as:

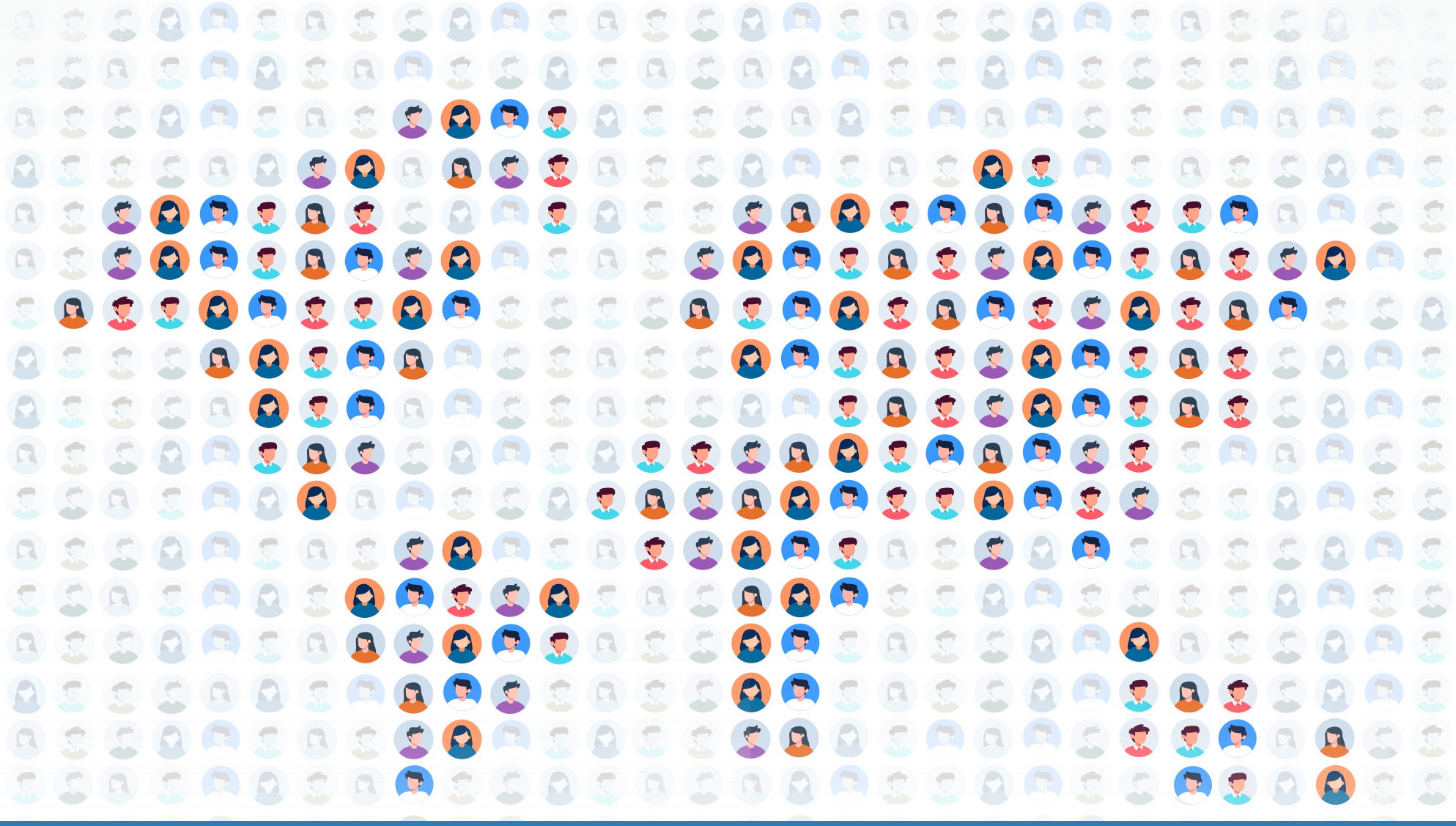


Facial Recognition

Artificial Intelligence

has further impact on the security and privacy. In conflict scenarios, these technologies can be used to **monitor large populations** with alarming efficiency, raising **ethical questions about their use.**

By increasing awareness and adopting robust security practices, it is possible to reduce the risks posed by hacking, phishing, and surveillance. However, as digital threats continue to evolve, so too must our strategies for addressing them in an ever-changing landscape of cyber warfare.



Maharat Foundation

Address:
Jdeideh, Metn
Beirut, Lebanon

Contact Information:
Website: maharatfoundation.org
Email: info@maharatfoundation.org

مهارات
Maharat