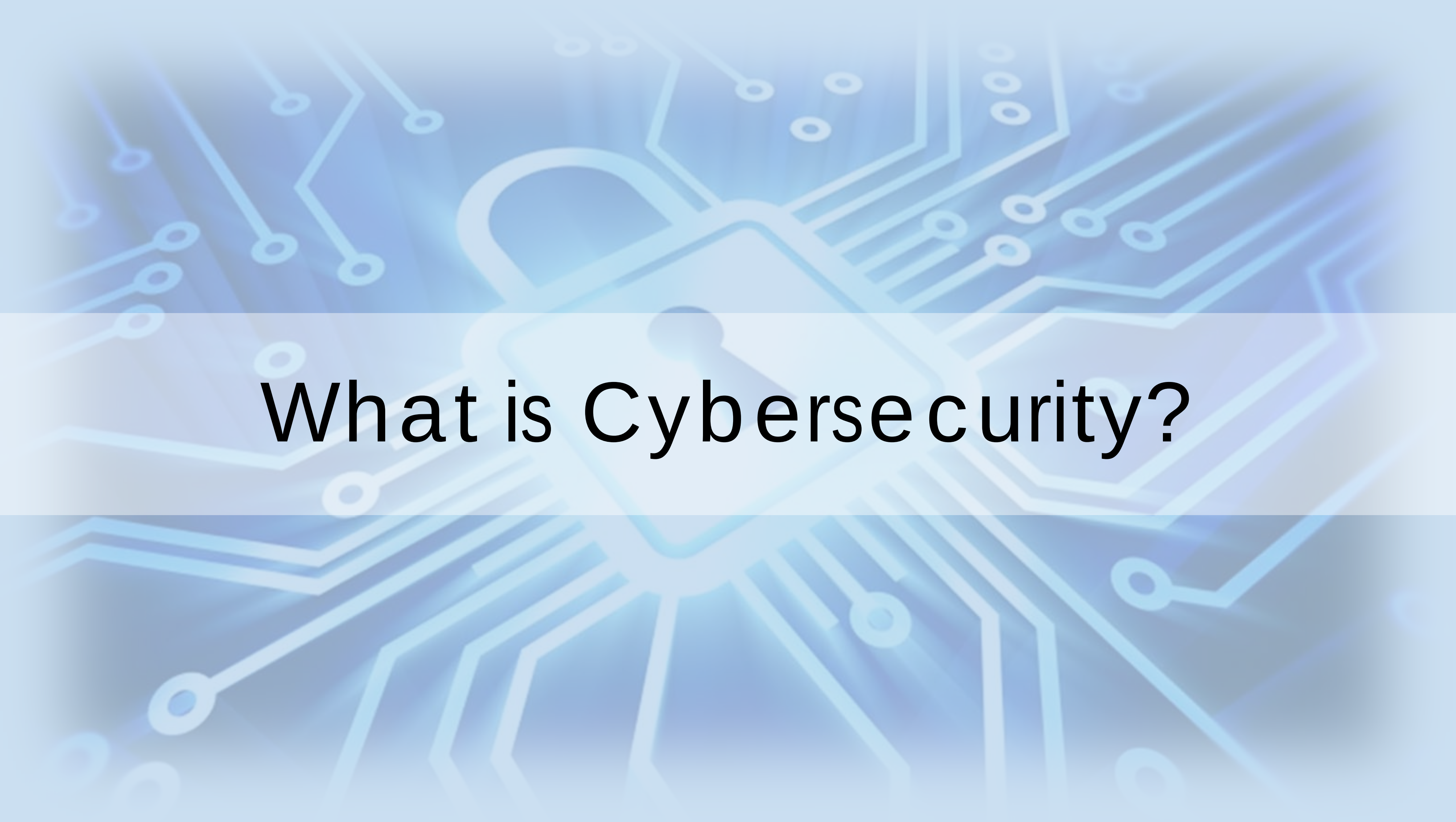
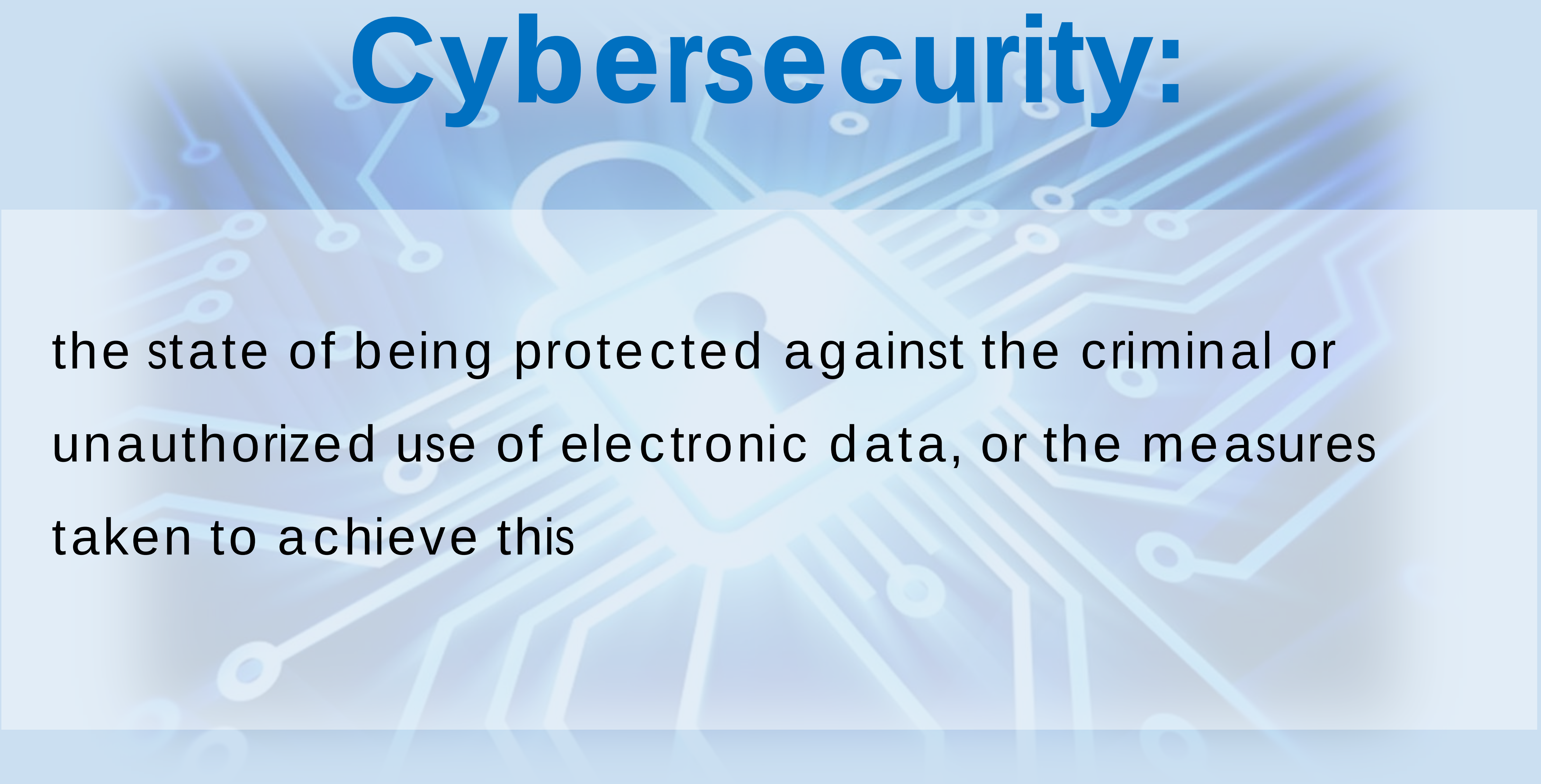
Cybersecurity

The Progression of Information Warfare

What is Cybersecurity?



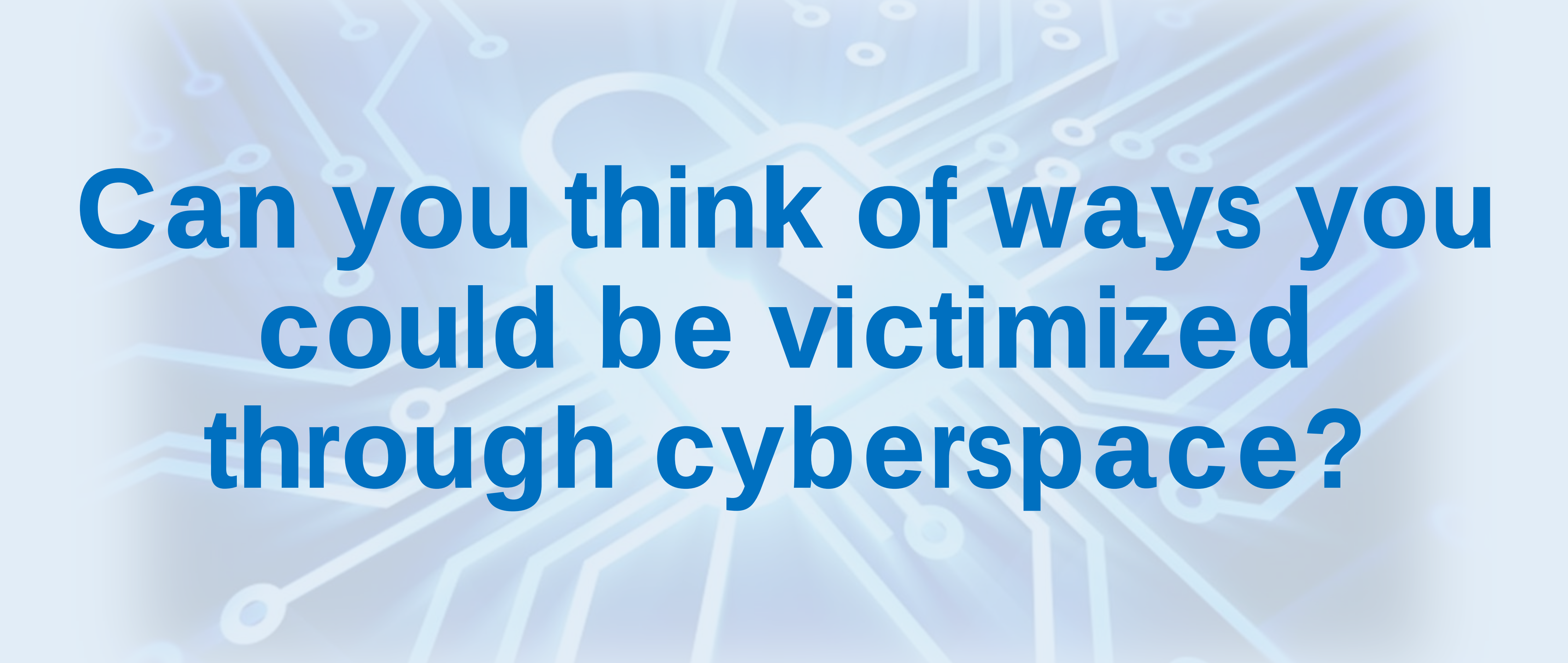
Cybersecurity:



the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

Information in the 21st Century

- So much of the information we use is now online or connected to a greater network
- We can exchange information in seconds
  - E-mails, texts, snapchats, Dropbox
- The ability to connect all this information allows the opportunity for information to fall into the wrong hands



Can you think of ways you could be victimized through cyberspace?

Cyber Victimization

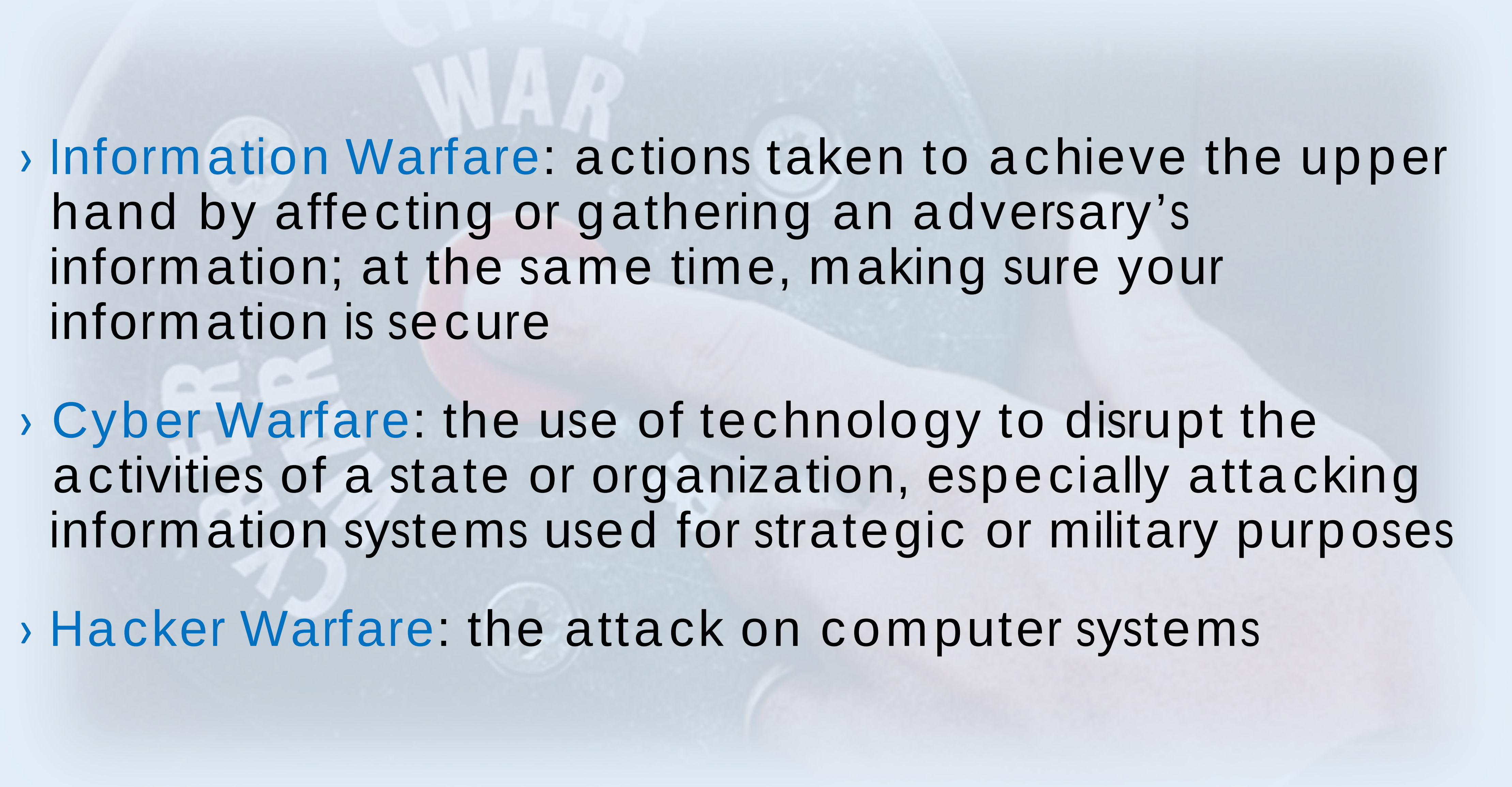
- You are affected by cybersecurity too! People can access your social media and other accounts.
- Cyberbullying
- Identity use on social media
- Use of your parents credit card information

Cyber Victimization

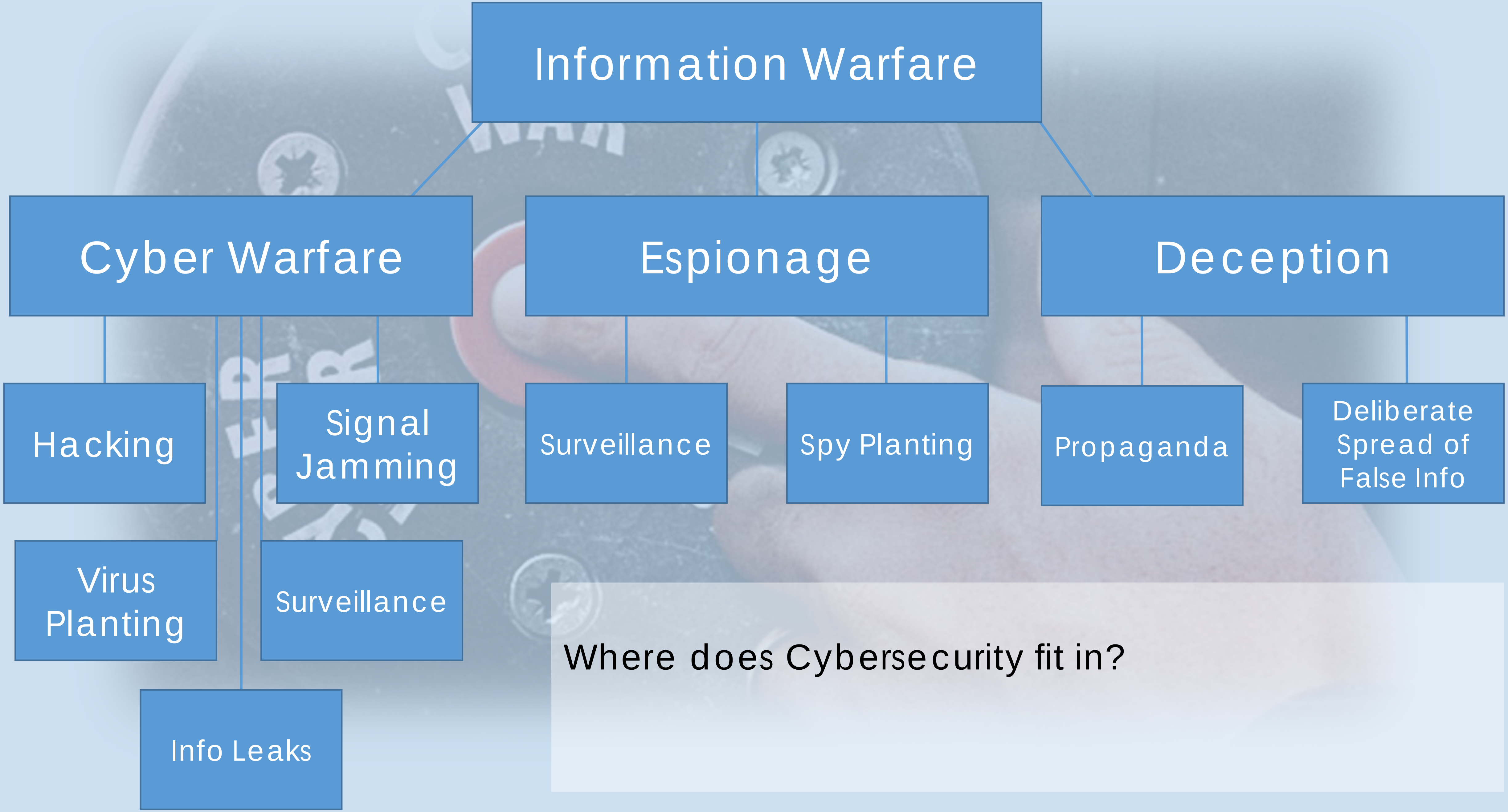
- Identity theft
  - The use of you or your parents social security number
- Credit card information use
  - Like the mass Target hack in 2013

Do you think cyber information can be used to harm more than just individuals?

Cyber Warfare

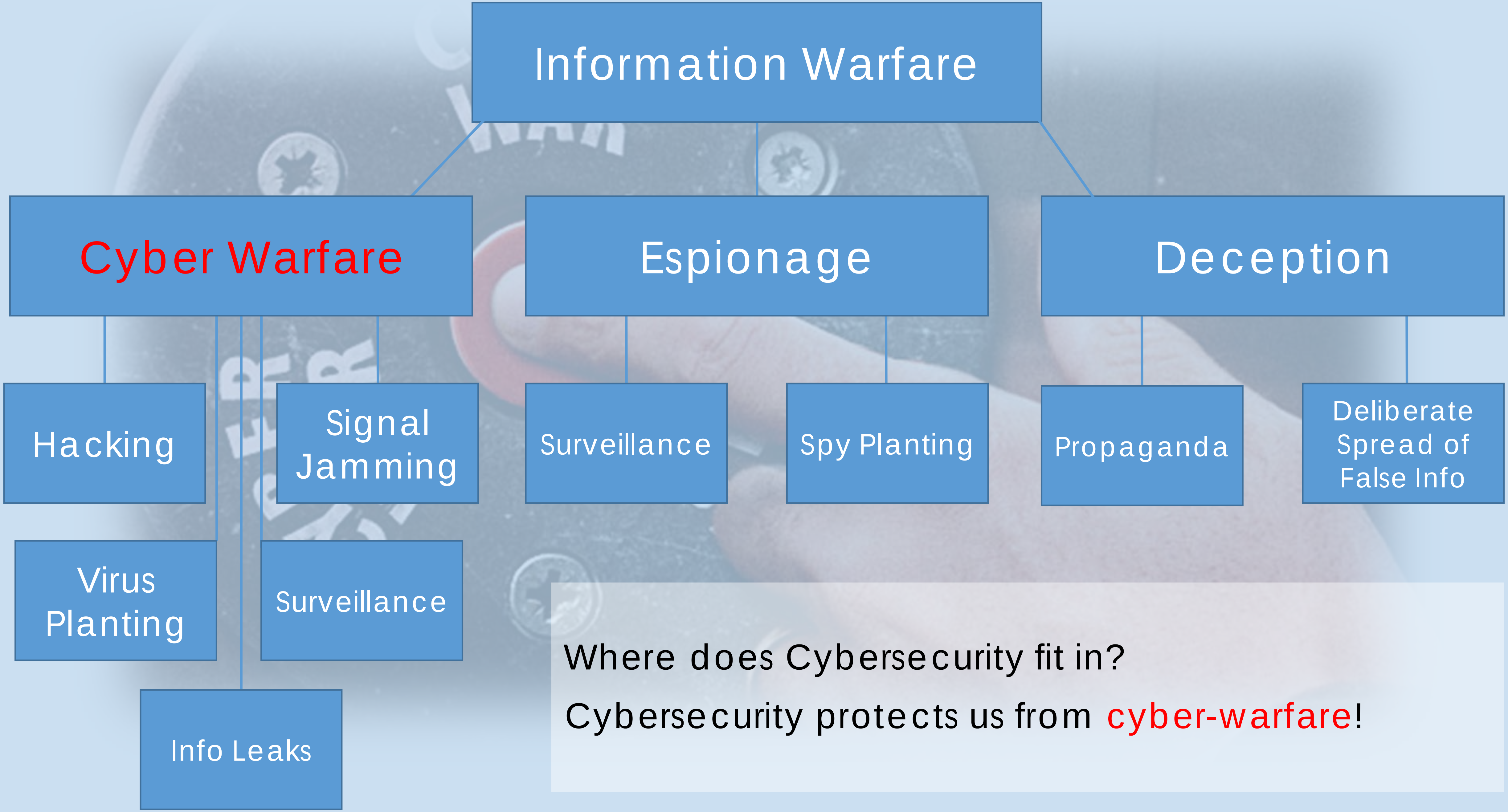


- Information Warfare: actions taken to achieve the upper hand by affecting or gathering an adversary's information; at the same time, making sure your information is secure
- Cyber Warfare: the use of technology to disrupt the activities of a state or organization, especially attacking information systems used for strategic or military purposes
- Hacker Warfare: the attack on computer systems



- Information Warfare
  - Cyber Warfare
    - Hacking
    - Virus Planting
    - Info Leaks
    - Surveillance
    - Signal Jamming
  - Espionage
    - Surveillance
    - Spy Planting
  - Deception
    - Propaganda
    - Deliberate Spread of False Info

Where does Cybersecurity fit in?



Information Warfare

Cyber Warfare

Espionage

Deception

Hacking

Signal Jamming

Virus Planting

Surveillance

Info Leaks

Surveillance

Spy Planting

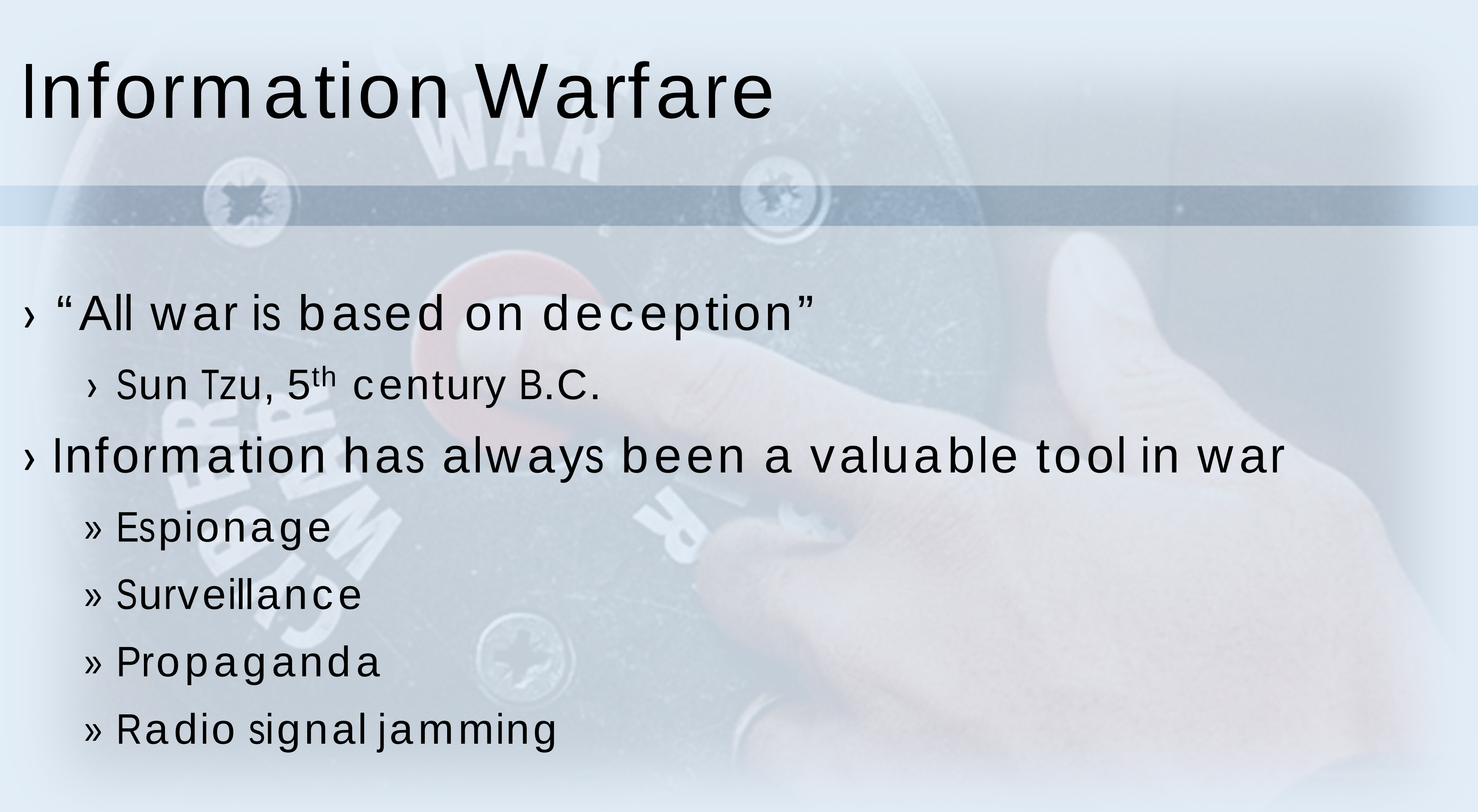
Propaganda

Deliberate Spread of False Info

Where does Cybersecurity fit in?

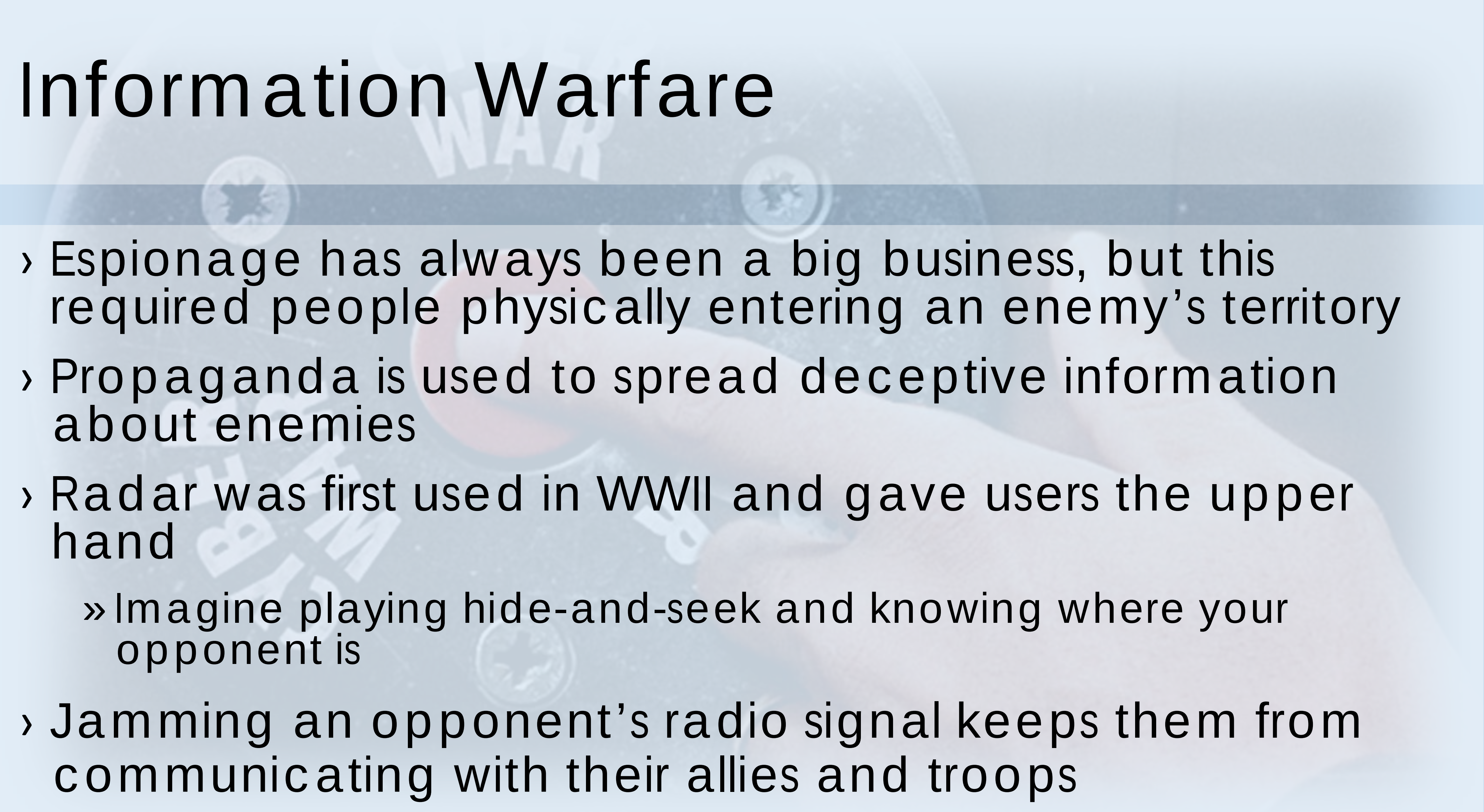
Cybersecurity protects us from cyber-warfare!

Information Warfare



- “All war is based on deception”
  - Sun Tzu, 5th century B.C.
- Information has always been a valuable tool in war
  - » Espionage
  - » Surveillance
  - » Propaganda
  - » Radio signal jamming

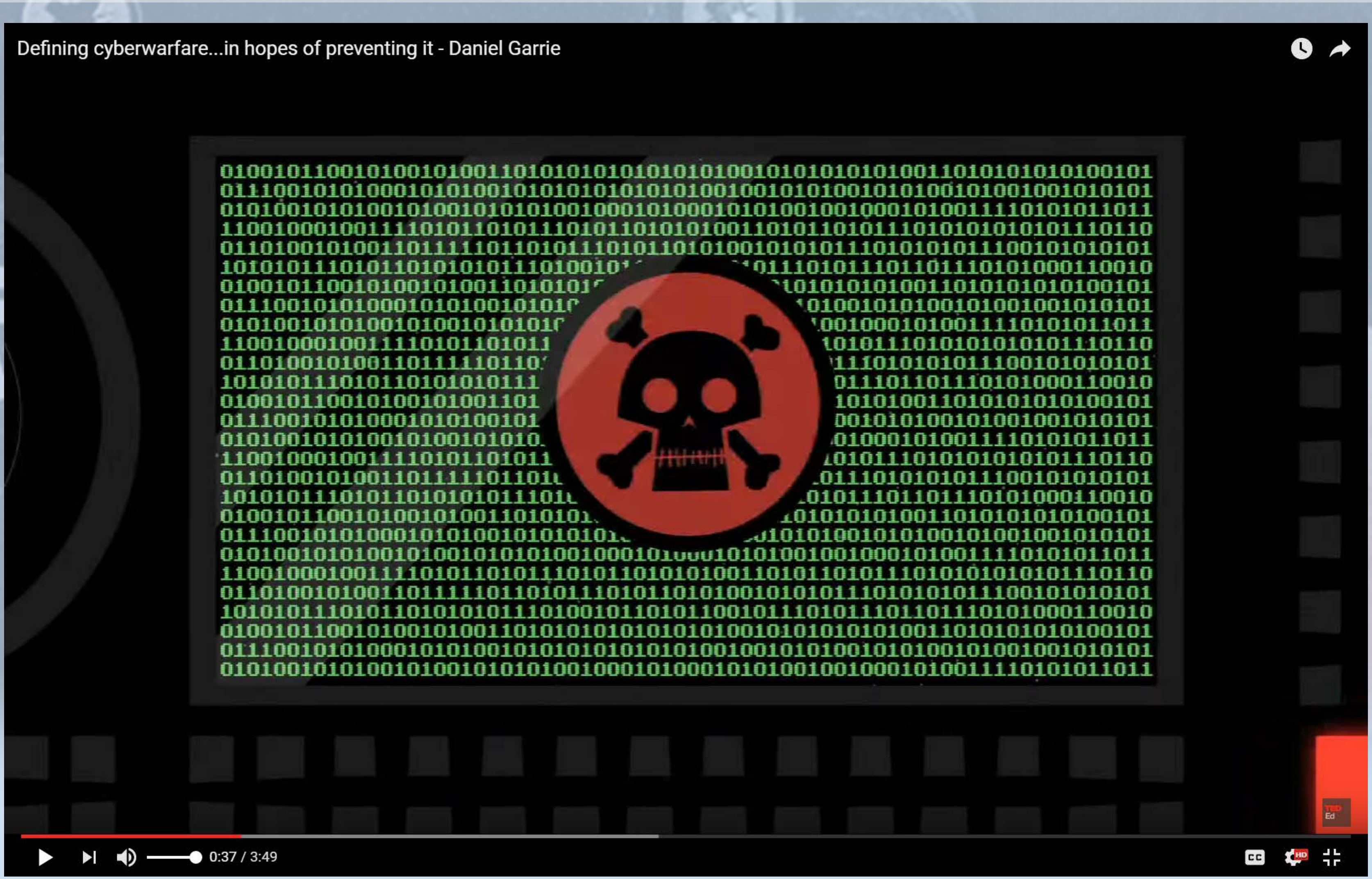
Information Warfare



- Espionage has always been a big business, but this required people physically entering an enemy’s territory
- Propaganda is used to spread deceptive information about enemies
- Radar was first used in WWII and gave users the upper hand
  - Imagine playing hide-and-seek and knowing where your opponent is
- Jamming an opponent’s radio signal keeps them from communicating with their allies and troops

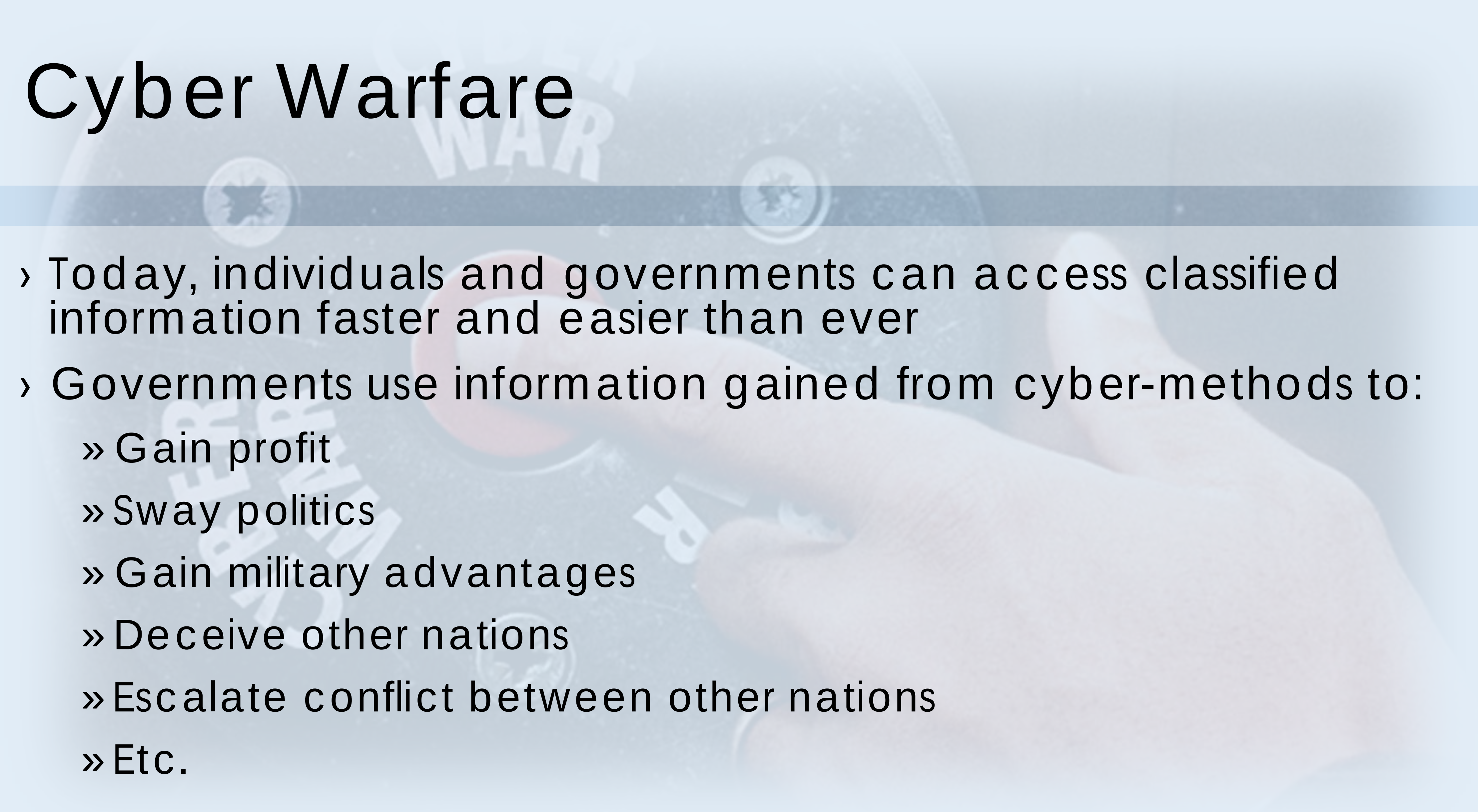
But cyber warfare can be so much more destructive…

Cyber Warfare



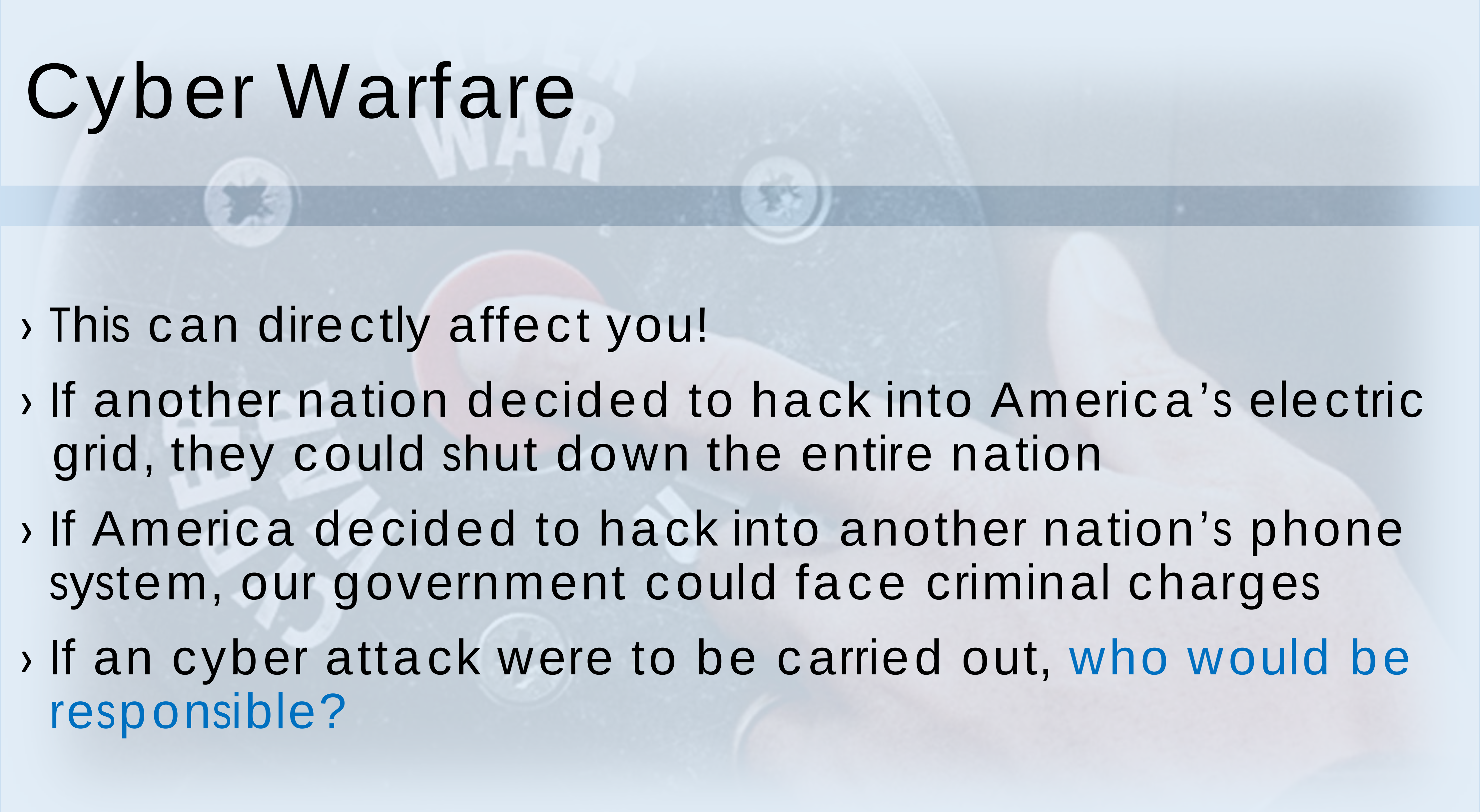
Defining cyberwarfare...in hopes of preventing it - Daniel Garrie

Cyber Warfare



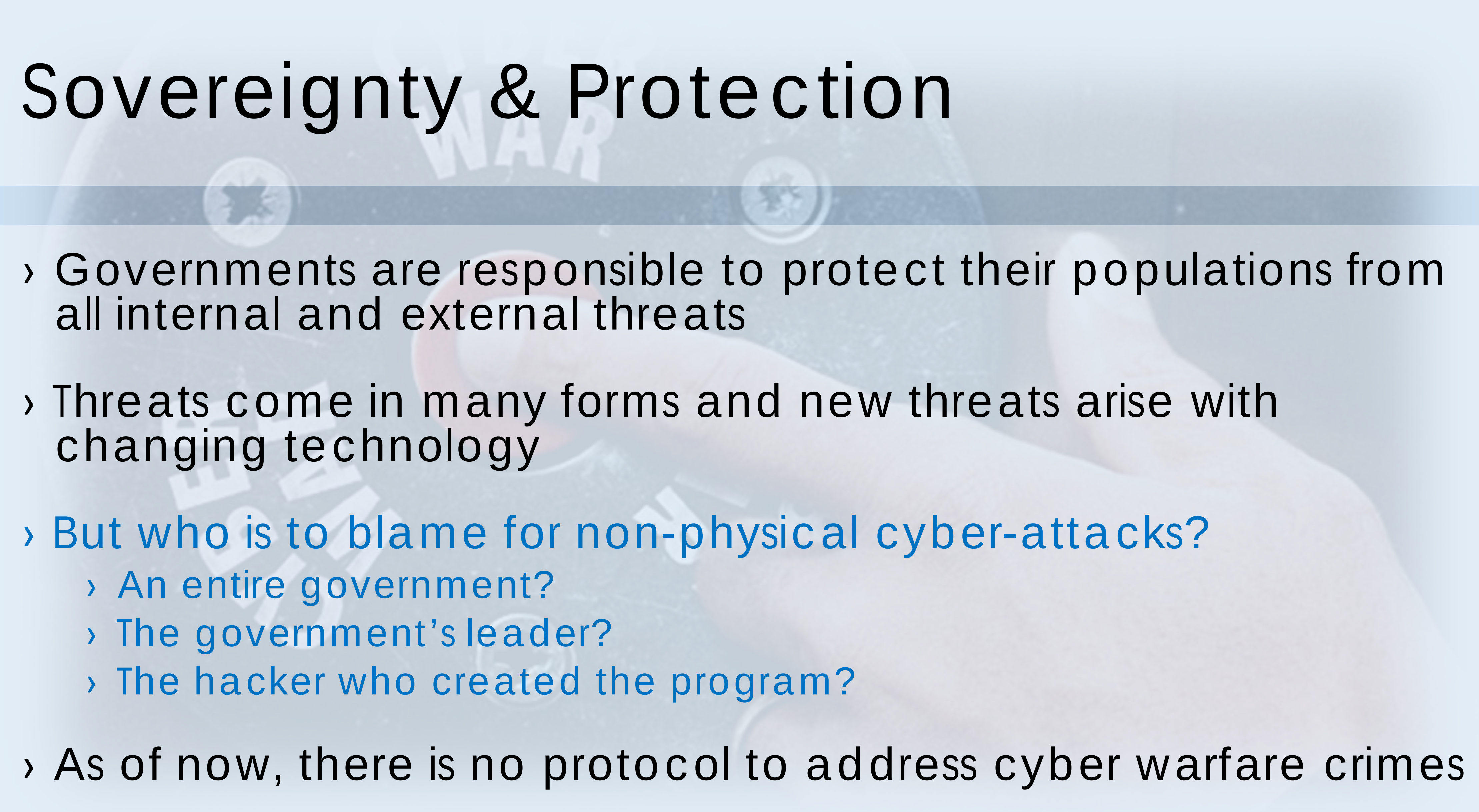
- Today, individuals and governments can access classified information faster and easier than ever
- Governments use information gained from cyber-methods to:
  - Gain profit
  - Sway politics
  - Gain military advantages
  - Deceive other nations
  - Escalate conflict between other nations
  - Etc.

Cyber Warfare



- This can directly affect you!
- If another nation decided to hack into America’s electric grid, they could shut down the entire nation
- If America decided to hack into another nation’s phone system, our government could face criminal charges
- If an cyber attack were to be carried out, who would be responsible?

Sovereignty & Protection



- Governments are responsible to protect their populations from all internal and external threats
- Threats come in many forms and new threats arise with changing technology
- But who is to blame for non-physical cyber-attacks?
  - An entire government?
  - The government's leader?
  - The hacker who created the program?
- As of now, there is no protocol to address cyber warfare crimes

Cyber Threats in the 21st Century

Stuxnet

- In 2009 the US and Israel launched a joint attack on Iran's nuclear facilities
- The virus, called Stuxnet, targeted the facilities' centrifuges and caused them to spin out of control and break
- Not only did this virus destroy the Iranian centrifuges, but it made the operators look incompetent
- Sources later claimed that the attack "changed global military strategy in the 21st century"

The Democratic National Committee

- In 2016, reports confirmed that two Russian hacking groups accessed the DNC's e-mails
- The hackers mimicked e-mail addresses in order to obtain classified information from party members and used existing information from the e-mails to leak restricted information
- By installing malware onto representatives' computers, the hackers gained access to important files on both government and personal computers
- As of now it is unclear whether the information was used to bias the election. What would the impact be if this were true?

WikiLeaks

- WikiLeaks is a multi-national media organization and associated library founded in 2006 by Julian Assange
- The site publishes censored and restricted data on official materials involving war, espionage, and corruption
- WikiLeaks protects people who send in censored information through its system of encryption

WikiLeaks

- One of the biggest controversies is the release of private emails from Clinton's campaign manger John Podesta
- Another WikiLeaks controversy involves the NSA’s alleged targeting of Assange
  - Documents claim to show that as far back as 2010 the US NSA added Julian Assange to a “MANHUNTING” target list, together with suspected members of al-Qaeda
  - The information revealed how the NSA collects information about American's phone calls, our email messages, our friends and contacts, how we spend our days and nights
  - Assange currently lives in Ecuador, who is offering asylum against possible prosecution in the U.S.

WikiLeaks

- WikiLeaks allows for transparency on governmental actions to an international community and for this reason has received criticism
- Some people view it as a legitimate source of information that ensures freedom of the speech, while others perceive it as unpatriotic and containing curtailed content
- Do you think classified information should be made public, as WikiLeaks promotes? What are the pros and cons?