New Technologies of Conflict : Policy Implication

General Jerdwut Kraprayoon

Agenda

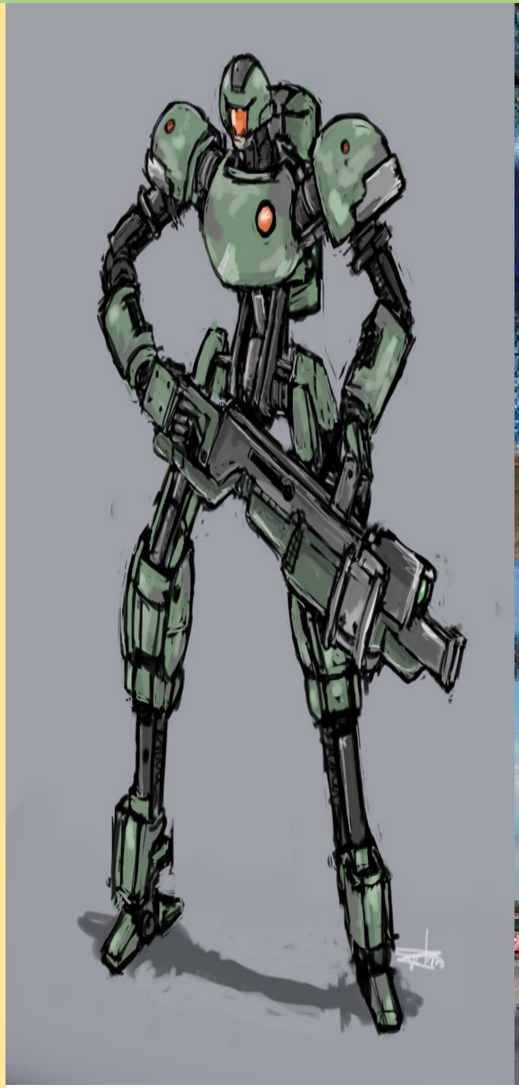
- Technology Disruption Age,
- Non State Actors with More Influential Roles,
- Sovereignty Implications,
- New Norms and Guidance,
- Analysis and Conclusion.

I. Technology Disruption Age

- Rapid Technological Change,
- Age of Uncertainty,
- Fore-sighting and Scenario Planning as a Norm,
- Nature of Conflicts: Changing Means, Econ, Tech, Social, Politics, Environment,
- Relies More on Other Means Than Military to Achieved National Objectives.

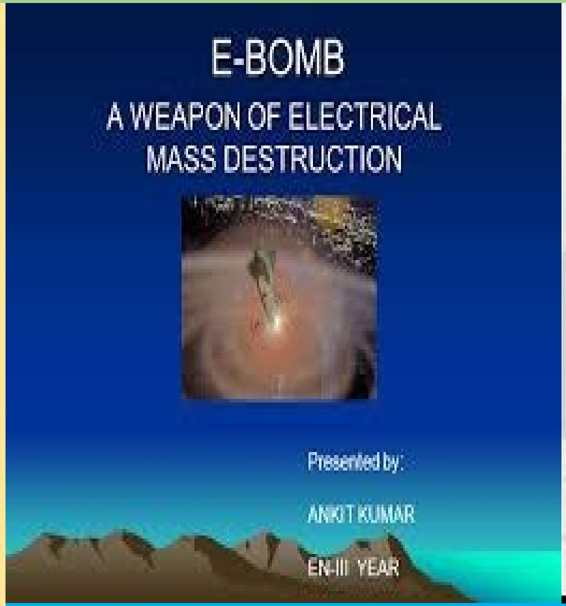
Potential Technologies of Conflicts (1)

- Autonomous weapons,
- High-energy lasers,
- Space-based weapons,
- Hypersonic aircraft,
- Active Denial System,
- Nuclear missiles,



Potential Technologies of Conflicts (2)

- Smart sensors,
- E-bombs,
- Layered missile defense,
- Information warfare (IO),
- Cyber warefare,
- Cyber security,
- Quantum supercomputer,
- AI (Artificial Intelligence).



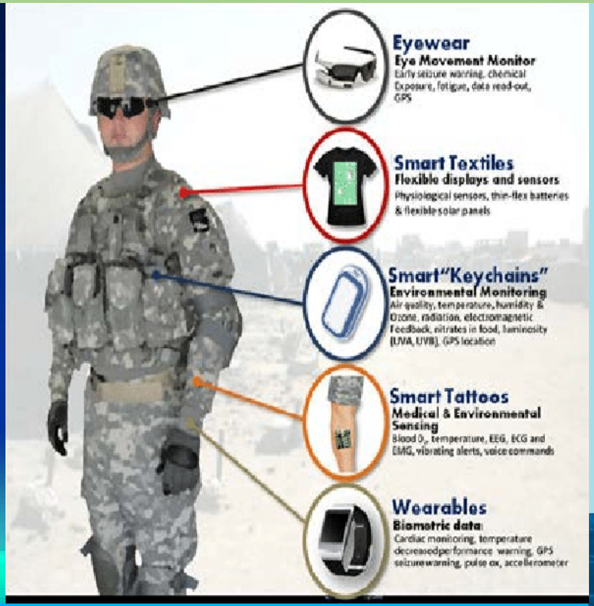
E-BOMB

A WEAPON OF ELECTRICAL MASS DESTRUCTION

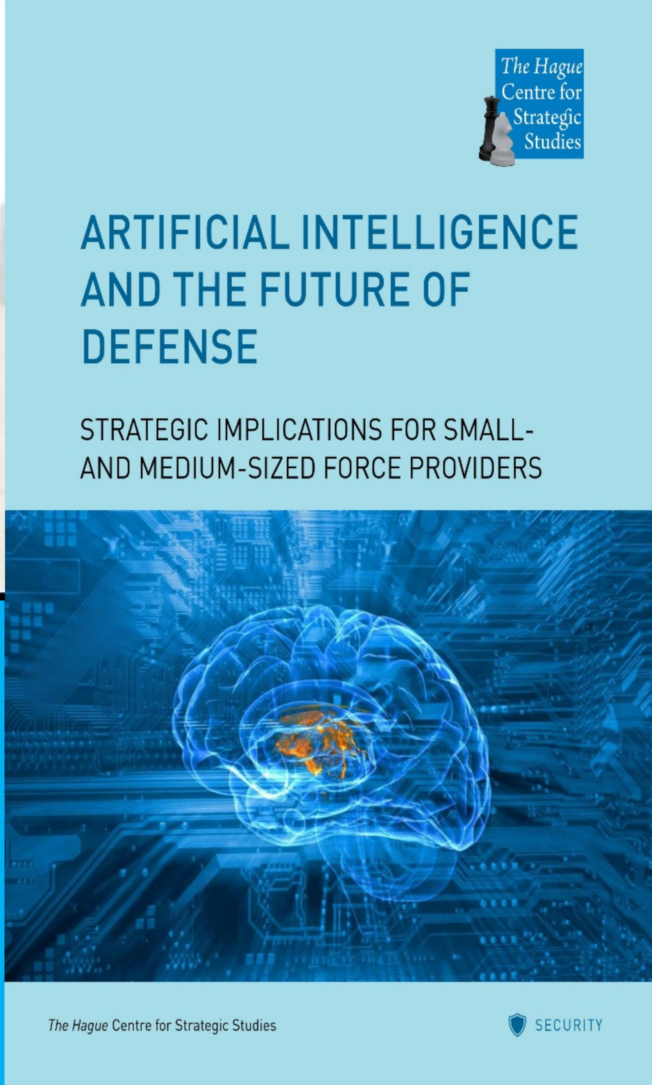
Presented by:

ANKIT KUMAR

EN-III YEAR



Eyewear
Eye Movement Monitor
Early seizure warning, chemical Exposure, fatigue, data read-out, GPS
Smart Textiles
Flexible displays and sensors
Physiological sensors, thin-flex batteries & flexible solar panels
Smart "Keychains"
Environmental Monitoring
Air quality, temperature, humidity & Ozone, radiation, electromagnetic Feedback, nitrates in food, luminosity (UVA, UVB), GPS location
Smart Tattoos
Medical & Environmental Sensing
Blood O₂, temperature, EEG, ECG and EMG, vibrating alerts, voice commands
Wearables
Biometric data
Cardiac monitoring, temperature decreasedperformance warning, GPS seizurewarning, pulse ox, accellerometer



The Hague Centre for Strategic Studies

ARTIFICIAL INTELLIGENCE AND THE FUTURE OF DEFENSE

STRATEGIC IMPLICATIONS FOR SMALL- AND MEDIUM-SIZED FORCE PROVIDERS

The Hague Centre for Strategic Studies

SECURITY

Quantum computing and defense

Potential military applications; National programs; Quantum supremacy

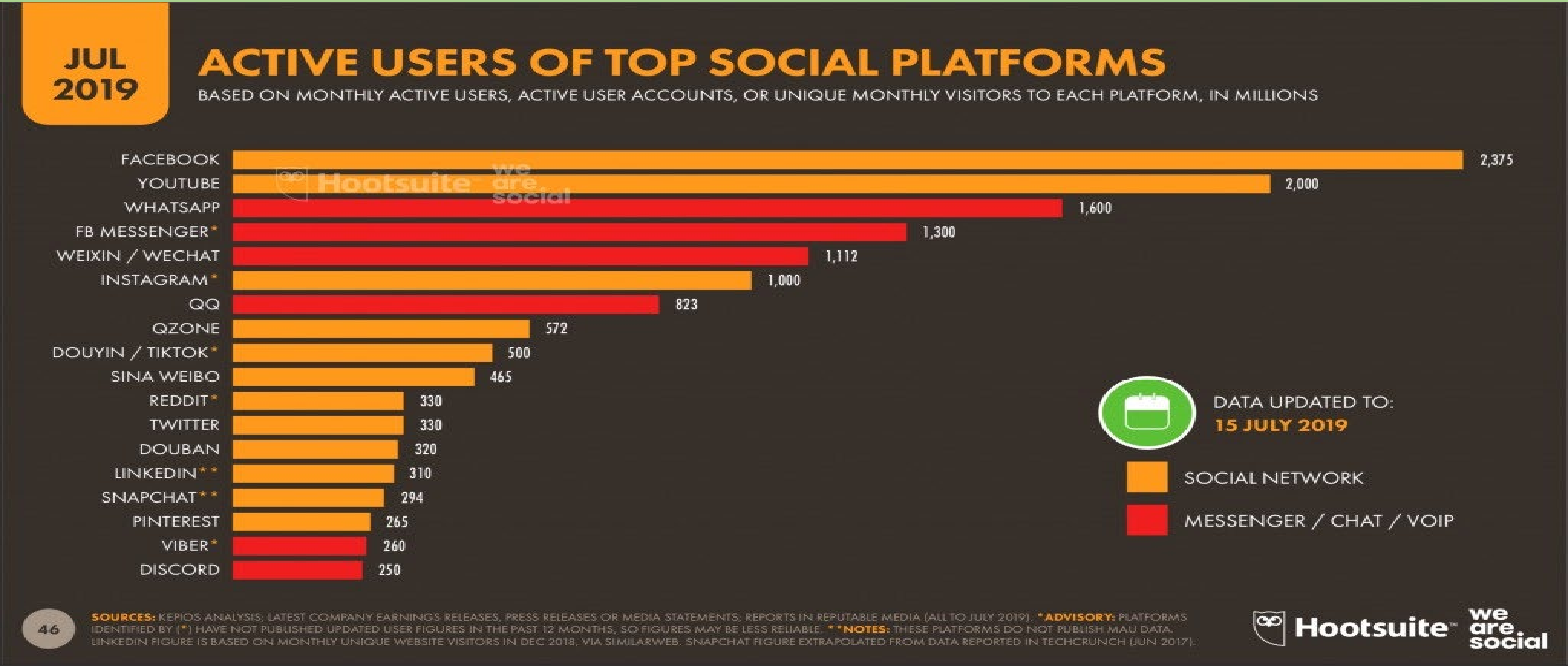
The Increasing Importance Role of Cyberspace

- Digital and Cyber is the Driver, Most Influencing Future of Conflicts and Peace in Several Aspects.

Separation of War and Peace time No Longer Exists

- A definite separation between war and peace no longer exists. Many crises have no clear beginnings and no definitive ends. The world’s most fragile countries are caught in cycles of instability, in which outbreaks of major fighting are interspersed with low-intensity violence and lawlessness. The U.S. itself has been fighting an open-ended war against al-Qaeda and its affiliates since 2001.
- Today, only rarely is war ever “declared.” The United Nations Charter, forged in the aftermath of World War II, limits the use of force—without a formal Security Council authorization—to self-defense. Self-defense is clear enough when troops cross a border. But what does “self-defense” mean when it comes to covert operations, unclaimed cyber attacks, “hybrid warfare,” or a terrorist strike launched from a failed state?

II. Non-State Actors with More Influential Roles



JUL 2019

ACTIVE USERS OF TOP SOCIAL PLATFORMS

BASED ON MONTHLY ACTIVE USERS, ACTIVE USER ACCOUNTS, OR UNIQUE MONTHLY VISITORS TO EACH PLATFORM, IN MILLIONS

DATA UPDATED TO: 15 JULY 2019

SOURCES: KEPIOS ANALYSIS; LATEST COMPANY EARNINGS RELEASES, PRESS RELEASES OR MEDIA STATEMENTS; REPORTS IN REPUTABLE MEDIA (ALL TO JULY 2019). ***ADVISORY:** PLATFORMS IDENTIFIED BY (*) HAVE NOT PUBLISHED UPDATED USER FIGURES IN THE PAST 12 MONTHS, SO FIGURES MAY BE LESS RELIABLE. ****NOTES:** THESE PLATFORMS DO NOT PUBLISH MAU DATA. LINKEDIN FIGURE IS BASED ON MONTHLY UNIQUE WEBSITE VISITORS IN DEC 2018, VIA SIMILARWEB. SNAPCHAT FIGURE EXTRAPOLATED FROM DATA REPORTED IN TECHCRUNCH (JUN 2017).

Influence of Cyber in Several Aspects

- Technology is often discussed in terms of its disruptive effect in fields from commerce to healthcare to education,
- Today, individuals are empowered by digital technology to have a voice in international affairs,
- Rapid innovation, particularly in ICT, has democratized the role of non-state actors in conflict and peacebuilding,
- ICT, from Facebook, Google to WhatsApp, helps people connect across borders and understand new perspectives, providing powerful tools for peacebuilders. "The fundamentals of peacebuilding are dialogue, facilitation, and mediation — enabling people to use their words to solve differences before they become violent,".

Increasing Role of Non-State Actors

- Technology is now disrupting governments and international affairs. The speed of innovation has left governments and international bodies struggling to keep up,
- Today's tech innovators are sidestepping governments and creating their own institutions, such as cryptocurrencies. "Nation-states are not leading interactions between citizens on the global stage,"

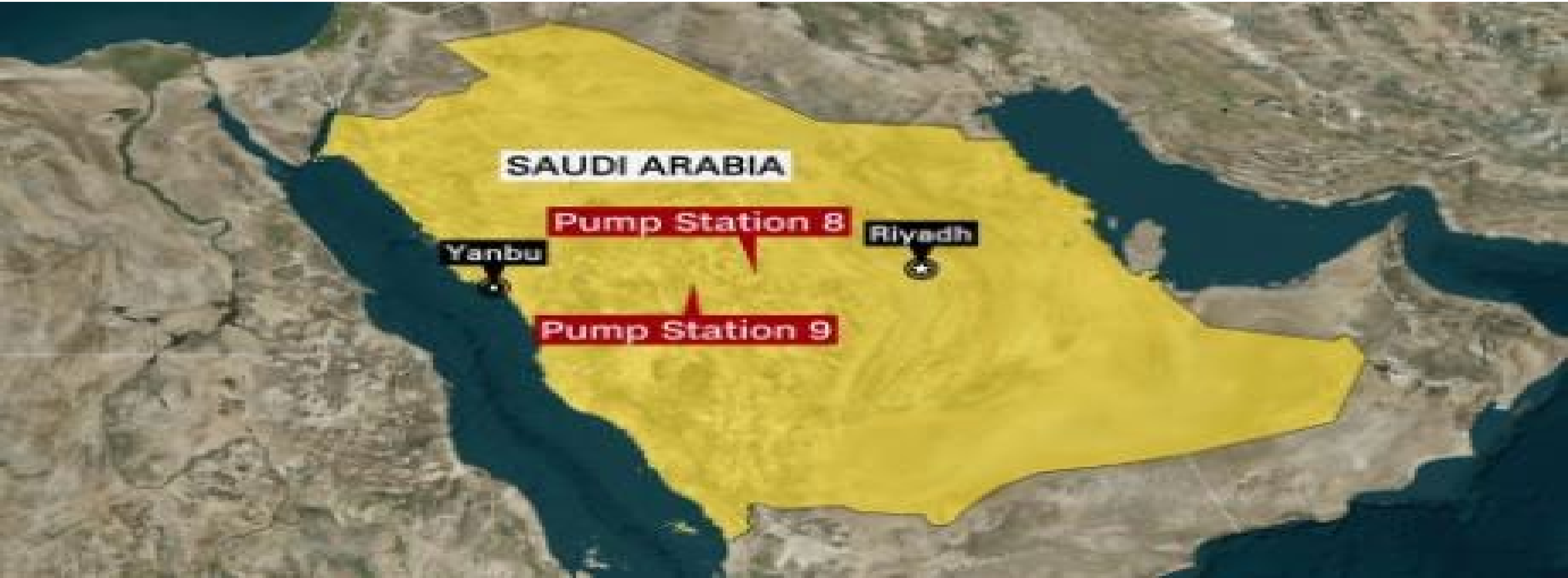
III. Sovereignty Implications

- Need guiding principle that govern the global cyberspace,
- China and US may have different narrative of how to apply cyber sovereignty principle to guide the governance of global cyberspace, both two countries pay special attention on how to ensure the cyber sovereignty in different ways. US prefer to expand its cyber sovereignty, while China prefer to launch the cyber sovereignty defensively,
- Cyber Sovereignty and Data Sovereignty,
- Some economic actors misunderstand the term "cyber sovereignty" as a form of autonomy in cyberspace. This Trend Analysis argues that using the term "cyber sovereignty" in the same way as "autonomy" is a misnomer,
- The research examines the debate on sovereignty in other domains: sea, air, and space. This showed that each domain went through discussions on the applicability of sovereignty, before the normalization of practices in international treaties.

Legitimate Responses for States and Non State Actors? (1) – Ukraine 2015 & 2016

Legitimate Responses for States and Non State Actors? (1) – Two Major Saudi Oil Installations Hit by Drone Strike in September 2019

- The drone attacks in Saudi Arabia have changed the nature of global warfare,



Cyber warfare case study

- “Russia’s government thus defines IW (Information Warfare) as a strategic war-winning force in its own right and as an indispensable weapon for the intelligence preparation of the battlefield over many years.”

IV. New Norms and Guidance

- R2P ?
- Cyber warfare case study, “Russia’s government thus defines IW (Information Warfare) as a strategic war- winning force in its own right and as an indispensable weapon for the intelligence preparation of the battlefield over many years.”

International Body and Protocol to Oversee Cyber Sovereignty Issues?

- Need new guiding principle that govern the global cyberspace,
- Cooperation Among Existing International Bodies and Tech Titans,
- Create New Bodies to Tackle More Efficiently with Cyberspace Issues;
    - Cases of National Cyber Security Committee and National Data Protection Committee.

Legitimate Responses for Internationals – UN High-level Panel on Digital Cooperation: A Proposal for International AI Governance

- UN High-level Panel on Digital Cooperation: A Proposal for International AI Governance,
- International Digital Cooperation must be underpinned by the effective international governance of artificial intelligence (AI). AI systems pose numerous transboundary policy problems in both the short- and the longterm. The international governance of AI should be anchored to a regime under the UN which is inclusive (of multiple stakeholders), anticipatory (of fast-progressing AI technologies and impacts), responsive (to the rapidly evolving technology and its uses) and reflexive (critically reviews and updates its policy principles). We propose some options for the international governance of AI which could help coordinate existing international law on AI, forecast future developments, risks and opportunities, and fill critical gaps in international governance.

R2P – Need New Framework to Tackle Cyber Warfare ?

- The **Responsibility to Protect (R2P)** is a global political commitment which was endorsed by all member states of the UN at the 2005 World Summit in order to address its four key concerns to prevent genocide, war crimes, ethnic cleansing and crime against humanity.
- The principle of the **Responsibility to Protect** is based upon the underlying premise that sovereignty entails a responsibility to protect all populations from mass atrocity crimes and human right violations. The principle is based on a respect for the norms and principles of international laws, especially the underlying principles of law relating to sovereignty, peace and security, human rights, and armed conflict.

V. Analysis and Discussion

- Warfare has been upgraded. The past few decades have seen an extraordinary technological change in conflicts and in military capabilities generally.
- Reportedly more than 100 States have established dedicated cyber-warfare units within their armed forces or intelligence agencies.1 These units help States fend off hostile cyber-operations targeting their national infrastructure and – though this might not be equally publicized – undertake such operations against an adversary.

V. Analysis and Discussion

- Nearly as many States are said to operate unmanned aerial vehicles (UAVs) for intelligence, surveillance and reconnaissance, and allegedly some 30 States already have or are developing armed UAVs.2 Military applications of artificial intelligence, nanotechnology and biotechnology are being actively devised and implemented.
- This technological shift has sparked an extensive debate about the adequacy of the applicable international law. – Existing R2P is not enough !!!
- Need More Active Roles of Regional Bodies such as ASEAN ?

Q & A

Thank you