Cyber and Space

I. Intro
II. Cyber attacks on satellites
II. Policy recommendations

I. Intro

The Project

- Bringing together experts from both the cyber and space security communities to explore connections between the two domains.

The Landscape

- Space components (especially satellites) have become an integral part of cyberspace.
- Commonalities between cyber and space:

1. Reduction in costs for entry
2. Resulting increase in the number of actors

➔ **As the interdependence between cyber and space grows, so does the disruptive potential of threats**

II. Cyber attacks on satellites (I)

1. GPS attacks

a. Jamming

Definition: "Creating a false GPS signal that overpowers the real GPS signal"

How GPS works
- GPS (Global Positioning System) is a system primarily used for navigational purposes by individuals, commercial entities, and the military
- A series of earth orbiting satellites continually broadcast radio signals with their location and the time (measured by atomic clocks) to a GPS receiver on the ground
– The GPS receiver detects the signals coming from satellites
➔ Once the GPS receiver has locked on to 4 different satellites, it can use this information to pinpoint its exact location as well as to confirm the time.

II. Cyber attacks on satellites (II)

How Jamming works

- The problem is that GPS uses radio waves, which are very weak
- Thus, radio waves are among the easiest to jam

➔ **The attacker uses a jamming device that directs an even stronger signal at the GPS receiver so that it overpowers the satellite signal.**

Key point

- In Jamming, the victim knows that he has been the victim of an attack because his GPS receiver does not work

Concerns

- Jammers are easily accessible online and can be used by criminals, terrorists, and states
- They can cost as little as $30

II. Cyber attacks on satellites (III)

Jamming attacks

1. Can take down mobile phone signals
2. Used by organized crime to steal cars and lorries carrying goods
3. Censorship

Case study

- North Korean jamming attacks on South Korea (2010, 2011, 2012)

II. Cyber attacks on satellites (IV)

b. Spoofing

Definition: "Deceive the GPS receiver into tracking counterfeit GPS signals"

How Spoofing works
- A jamming attack comes first, in which the signal is overwhelmed
- The GPS receiver can no longer read the signal; it loses the lock on the satellite
- A perpetrator can use a satellite simulator to generate a fake GPS signal
- The GPS receiver then picks up the nearest signal

Key point
- In jamming, the target knows he has been a victim of an attack
- In Spoofing, the target does not know that the signal his GPS unit is receiving is a fake one
- Spoofing is therefore a way to feed false data into a system

II. Cyber attacks on satellites (V)

Doomsday scenarios: use by terrorists

- GPS is pervasive in everday life
- The perpetrator of a spoof attack can create a GPS signal that gives the incorect time to the intended receiver
- Because critical infrastructure depends on accurate time, it would be possible to:

1. Cause part of the power grid to explode
2. Interfere with the functioning of banks and stock exchanges
3. Disrupt civil aviation systems, law enforcement, and emergency service communications

II. Cyber attacks on satellites (VI)

2. Bringing down a satellite

Case study: Ukraine attempts to take down a Russian satellite (March 17th)

-This can be done by sending a signal from the ground that causes a satellite to manoeuver and lower its orbit

- This could push it to re-enter the earth's atmosphere and burn up

3. Eavesdropping

III. Policy recommendations

1. Methods to strengthen GPS

2. If atomic clocks become less expensive, this would reduce problems with jamming of mobile phones, among other issues

3. Possibility of using eLoran as a complementary technology