ECIPE PRESENTATION » 07.03.12

ONLINE WARFARE & INTERNATIONAL RELATIONS

Hosuk Lee-Makiyama
Co-Director, European Centre for International Political Economy (ECIPE)

International political economy of internet

- **Assumption that cyber security is "the most serious economic and national security challenge we face as a nation"…**
  - …modern societies are 'not prepared', 'ridiculous to suggest anything else'
  - Dissemination beyond the pace of domestic and international regulation
    - Half bn people joins the internet before a national legislation can be passed
    - China being the largest internet economy in the world since 2008
- **…or uneasiness, concern about moving from a uni- to multipolar world**
- **… leading vulnerability of open and connected societies:**
  - Center for New American Security claims approximately 1.8 billion cyber attacks of varying sophistication targeting Congress and federal agencies each month
  - $300 billion worth of trade secrets are stolen on annual basis in the United States, according to the US Cyber Command
  - Not an US-centric issue; In China, cyber-attacks doubled between 2011 and 2012
- **… or overselling the threat of internet on foreign policy**
  - Does the debate exaggerate soft powers and digital diplomacy
  - At the height of Arab Spring, less than 15 000 registered users of twitter in Egypt, Yemen and Tunisia
  - Surprising share of population in favour of government internet control

» Ethics of war – yet few occasions qualifying as ‘war’

- **Realist’s worldview has dictated collected policy response:**
  - “The next Pearl Harbor is likely to be a cyber attack going after our grid
    - *Leon Panetta, then CIA director now Secretary of Defence*
  - “Attacks against networks that control the critical infrastructure in this country could wreak havoc”
    - *Denis Blair, Director of National Intelligence*
  - » Real-time response simulations show they ‘pose genuine threats’ to telco networks, electricity grid & trading
  - » Online security now a part of the defence doctrine
    - US establishing a ‘cyber command‘
    - Now part of strategic concept of NATO (Lisbon Declaration 2010)
- **As of yet, there are very few cases of ‘pure’ cyber warfare.**
  - » Cyber-terrorism’, ‘-crime’ or ‘-espionage’, and no clear-cut case of outright wars:
  - » Only two close calls (out of supposed billion cases per month):
    - Estonia targeted in 2007 for three weeks by allegedly state-sponsored Russian hackers, though this was never proven. Using DDoS-attacks, the cyber-attacks targeted the websites of Estonian parliament, government ministries, political parties, media and banks
    - 2008 South Ossetia War, Georgian news media websites were targeted by (allegedly) state-backed Russian hackers. Government websites moved to Blogspot
- **No evidence to date that a sovereign state can be durably paralysed by cyber-attacks or can lose a war in cyber-space**
  - » End-users may face potential cyber-security issues, however cyber-incidents that affect entire networks or critical infrastructure are quite uncommon
  - » Question whether openness as a threat or acting as deterrent?
- **Why refer to ‘cyber threats’ as war?**

» Asymmetrical threats leading to disproportionate response

- **Online threats follow the pattern of all asymmetrical threats**
  - » Like all **asymmetrical** threats, levelling the playing field between the hegemonic and emerging/marginalised powers or **non-state actors** (NSAs)
  - » Which presents a threat with non-existent **defence capabilities**
  - » No deterrence from **retaliation**
    - No mechanism like the nuclear deterrent (mutually assured destruction) leading to START I/II talks
  - » 'Known unknowns' unleashing disproportionate political and popular responses
- **Like asymmetrical threats, 'cyber war/terrorism' not governed by international law**
  - » **Rule of war** (Hague convention, Geneva Conventions) inapplicable, aggression or behaviour between sovereign states and armed forces
  - » No concept of 'just war' — neither jus ad bellum or jus in bello
  - » Non-binding language of co-operation in **international treaties**, so far never put into practice
  - » Governed by unilateral or **extraterritorial application** of national law (cf. maritime law)
- **Reactions dispersing borders between culture, international trade and telecommunication**
  - » Open networks perceived as a strategic resources, view of internet as a deployable asset
    - Concept of information sovereignty
  - » Action and response targeting commerce rather than government or personal entities
    - Increasing classification of 'strategic' or 'vital interests' especially in a time of crisis
- **W(h)ither multilateralist order?**
  - » UNSC/UNGA, OHCHR, UNESCO, ITU, WTO/UNCTAD, WIPO, IGF … INTERPOL

» Commerce and internet security

- **Stuxnet incident, 2010**
  - » Allegedly caused the processing units in Iranian nuclear facilities in Bushehr and Natanz to spin out of control and self-destruct, thereby delaying Iran's ability to develop nuclear weapons.
  - » Stuxnet infected several controller equipment designed for use in industrial automation made by a German manufacturer
- **Operation "Aurora", 2010**
  - » Google announced that it "detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google"
  - » Google stated: "Primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists", Google withdrawing (or not) from Mainland China
  - » However, the attack also aimed to gain the proprietary source codes from United States companies and resulted in intellectual property theft in commercial banking, chemicals, software and ICT devices manufacturing
- **Target, accomplice or both?**

» Policy response: Balkanisation, decoupling interdependencies

- **» Going offline**
  - Great Firewall of China or liquid cement
  - State monopolies e.g. news mediation, including financial news (Thomson Reuters)
- **» Investment restrictions**
  - Cttee on Foreign Investments in US (Cfius) against Huawei, ZTE
    - *2008: Huawei forced to give up 16.5% stake bid in American network equipment maker 3Com*
    - *2010: Huawei and ZTE excluded from bidding for large network contracts from Sprint Nextel (even though the companies offered better terms than their competitors)*
    - *2011: Huawei forced to give up plans for $2 million purchase of patents from Californian start-up 3Leaf*
  - Ban of Chinese handsets in India
  - Foreign equity caps on investments in telecoms (China, US, certain EU member states)
- **» Scrutiny of state-owned enterprises and subsidies**
  - The EU-China megaphone diplomacy of 2012
- **» Indigenous innovation (China, India)**
  - Forced surrender of source codes and other forms of intellectual property
- **» Control of public procurement (MLPS)**
  - The scheme covers 60-70% ($35.2-$41.0 billion) spent on ICT in the public and private sector
  - Health care, education, finance and banking, energy, telecoms, insurance and transportation fall under the purview of the MLPS
- **» Data localisation rules or local content requirement**
  - ICT equipment in India, 80% of domestic demand to be met by local producers
  - Blackberry in Saudi Arabia, UAE
  - Safe harbour under EU DPD
- **» Encryption**
  - Ban of foreign encryption technology in China, India

» Diplomacy and ethics

- **First, it starts with a misguided assumption or consensus of the commentariat:**
  - » “Oppressive regimes would never be able to control the internet” – but No “End of History” in sight
  - » No clean or arithmetic link between online/economic development and more ethical societies (modernisation theory)
- **Second, ethics is not a vital objective of digital foreign policy:**
  - » Geopolitics today largely shaped by economic statecraft
    - The increasing market competition between countries rather than individual companies put ‘economics back at the heart of their foreign policies‘ — ‘The US global leadership and economic strength is packaged deal’ that feed from each other
  - » Coalitions or behaviour not based on aligning views on normative behaviour, morals or ethics
- **Third, digital diplomacy for open internet has so far failed:**
  - » From Haystack episode to ‘arming’ NGOs on the ground
  - » Reciprocated scepticism against open internet by legitimate and democratic governments
    - France in G8 Deauville
    - WCIT against the multi-stakeholder model
    - First cases of extraterritorial application of censorship starting in Europe
  - » Failure of economic sanctions, embargoes
  - » Lack of leverage from ‘European values’ and strategic partnerships
- **Fourth, unethical behaviour by states not (cannot be) addressed:**
  - » Sovereign, national interests before human interests
    - Liberal morality and ethical dilemmas of foreign policy shaped in 1960/70s
    - Theories questioning realist thought on individuals and states
  - » Limited success of theoretical principles or universalism:
    - UN Charter, Universal Declaration of Human Rights
      - *Unenforceable, largely incapable of addressing political and religious censorship off & online*
    - Erga omnes

» No ethical balancing but an economic diplomacy of proportionality?

- **Traditionally no ethical considerations in international economic policy or law**
  - » Conditionality in trade agreements, impractical or without effect
- **World Trade Organization (established in 1994) following GATT (1947)**
  - » Dispute settlement enforced through settlements and trade retaliation
  - » There is no ethics test in trade law
    - General exceptions (GATT art XX; GATS art XIV) for maintaining public morals and public order
    - …given no '**arbitrary**' and '**unjustifiable**' discrimination, but jurisprudence provides that Members are free to set whatever moral standard they like (China—audiovisuals)
    - Technical barriers to trade **not more restrictive than necessary** to fulfil a legitimate objective (incl. national security), taking account of the risks non-fulfilment would create
    - Security exceptions (GATT XXI; GATS XIV bis)
      - *Military contracts, limiting disclosure of security interests*
      - *Measures in times of war and emergency in international relations*
      - *Obligations under the UN*
- **Closest resemblance of ethics test in foreign policy: Proportionality under trade law**
  - » Objective at discretion of members but
    - Must show that '**genuine and sufficiently serious** threat is posed' to '**fundamental interest**' of society
    - **Necessary** for moral, order or national security
    - **Least restrictive measure** reasonably available for the level of morals pursued — genuine alternatives
    - Established in case law over Korean restrictions on beef, US online gambling, Chinese audiovisual products
  - » Enforceable: close to 100% compliance rate but some inherent weaknesses
- **Cyber security actions/responses as hidden trade barriers**
  - » Primary an economic (protectionism) or civil security problem
    - Re-dressed as a foreign policy instrumentation?