Towards digital insecurity? Cyber conflict, cyber meddling and the prospects for cyber peace

Engagement with Young Diplomats,
Ministry of Foreign Affairs, Nay Pyi Taw, Myanmar

Outline

1. Cyber conflict
   1. Definition & empirical puzzle
   2. Empirical findings: what kind of cyber conflicts are there
   3. Explaining levels of cyber conflict
2. Cyber meddling
   1. Definition & examples
   2. The German Netzwerkdurchsetzungsgesetz 2017 (Network Enforcement Act)
3. Conclusion

Step 1

Cyber conflict

Cyber conflict: definition

- Cyber conflicts may be defined as „incompatibilities of interests of at least two actors which shape their behavior and are directed to impair another actor by means of information and communication technology (Steiger et al. 2018: 8).“

Cyber conflict: Empirical puzzle & research questions

- Empirical puzzle:

1. Cyberspace is becoming an increasingly competitive domain for governmental and non-state actors.
2. However, the often quoted “World-War-C” has not occured (e.g. Geers et al. 2014).
3. Instead, we find considerable evidence for cyber- self-restraint.

- Questions:

1. How can we explain limited cyber conflict behaviour?

State restraint in age of „cyber war“

- Several authors have suggested that state government's, despite their significant technical capacities to attack, engage in cyber *self-restraint* (e.g. Valeriano/Maness 2014; Rid 2013).

- <u>Possible explanatory factors:</u>

➢ Fear of retaliation
➢ Fear of escalation and consequential collateral damages
➢ Shared norm(s) of (state-)responsibility

- <u>Genuin cyber-related aspects with relevance:</u>

➢ Attribution problem
➢ Use-and-lose-logic
➢ Replicability of attack codes

Empirical results from Heidelberg Cyber conflict index: HD-CY.Con

- Cyber-conflict research still lacks far behind conventional conflict studies (cf. COW, UCDP, HIIK): exception Valeriano/Maness 2014.
- Based on this, the HD-CY.Con is developed as a comprehensive cyber conflict dataset, including following characteristics:
  1. The dataset includes state- and non-state actors as initiators.
  2. The data set tracks attacks/counter-attacks against (commercial) targets when they become politicized.
  3. Chinese and Russian sources are analysed to control for cultural/political selection bias.
  4. The intensity measurement was developed inductively.

First preliminary findings

Valeriano/Maness 2014

Table V. Summary of cyber conflict among rival states (2001–11)

Rival A (number initiated)	*Rival B (number initiated)*	*Cyber incidents*	*Cyber disputes*	*Most severe dispute*
China (20)	USA (2)	22	5	3
Pakistan (7)	India (6)	13	3	3
North Korea (10)	South Korea (1)	11	3	2
Israel (7)	Iran (4)	11	2	3
China (7)	Japan (0)	7	7	3

HD-CY.CON/
Steiger et al. 2018

State A	State B	* Initiator: state	Initiator: state-sponsored	Initiator: hacktivist(s)	N	Intensity
India (4)	Pakistan (14)	1	1	16	18	1
Russia (7)	USA (1)	1	5	2	8	1,25
Russia (6)	Ukraine (1)	5	1	1	7	1,6
Korea (0)	North Korea (5)	3	2	0	5	1,8
Iran (2)	Saudi-Arab. (2)	0	1	3	4	1,5
Total		10	10	22	42	1,4

**Based on the respective attribution.*
***Total: 321 Incidents (2014-2016); Intensity scores range from 1 to 15.*
****Number of initiated attacks in brackets.*

Due diligence as an emergent (global) norm?

Responsibility is the accountability of an actor for the consequences of his action in relation to an applicable norm (cf. Heidbrink 2016: 5).

Prospective responsibility: expectation-driven responsibility for norm-enforcement itself.

→ *Due Diligence in Cyber-Space: „Obligation to warn“ (Corfu Channel 1949); „Do-No-Harm“ (Trail Smelter 1941); „No-Intervention“ (Nicaragua-sentence 1986).*

Retrospective responsibility: accountability for the intended and unintended consequences of the behavior (Erskine 2003: 8).

→ *Articles of state responsibility by the ILC (2001).*

→ *UNGGE Report 2013 & 2015.*

States as Cyber norm entrepeneurs

	USA	China	Germany/EU
National	**Critical Infrastructures as** „national strategic asset“ (National Security Strategy 2017)	**Comprehensive security-standards:** → Access to private and commercial networks → Digital state sovereignty	**Strong data protection legislation** IT-security-law 2015: → Protection of critical infrastructures
Bilateral	Joint communiqué by G20 (incl. China) **Cyber-espionage agreement with China (2015)**	**SCO-Treaty on Information Security (2009)** Cyber-security agreement with Russia (2015)	EU-Cyber-security-strategy 2013 **Data protection:** **→ Privacy Shield (2016)**
Multilateral	**International Strategy for Cyberspace (2011)** - Multi-stakeholder-approach at UN level - Norm breach by NSA	**Principle of intergovernmentalism at UN level** Application of international law to cyberspace	**Multi-stakeholder approach at UN level** Lead of UNGGE 2016

Conclusion

- Findings

1. Self-restraint appears to have a strong influence on state and non-state-actors. „Cyber Pearl Harbor“ has not taken place so far.

2. The Due diligence norm is still in its infancy in the cyber context.

3. By using non-state actors as proxies, states are undermining the regulative effect of the sovereignty/no-use of force norm in cyber space.

4. Global hacktivist groups, such as Anonymous, conduct primarily low-level attacks, either because of a lack of resources/competences (less likely) or because they prefer politicization over militarization.

5. Cyber-specific characteristica (use & lose logic, replicability and escalation risk) may explain the low mean intensity score for coded cyber incidents.

Step 2

Cyber meddling

Cyber meddling: definition

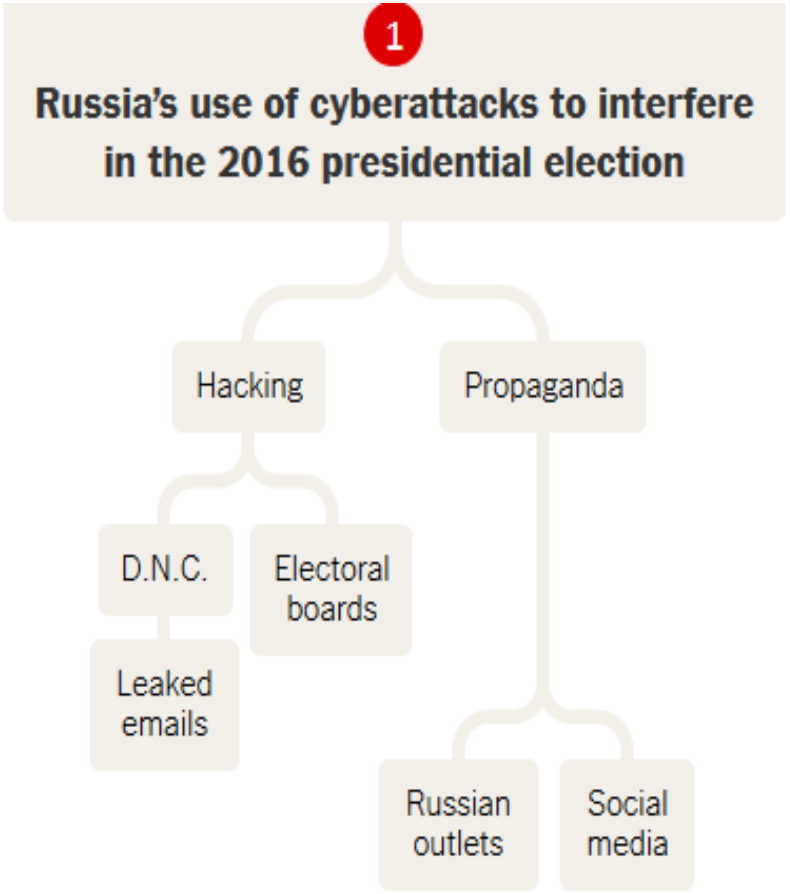
- Cyber meddling may be defined as an „international wrongful act“ (a breach of a legal obligation owed by one State to another under international law and attribution of the act to the former) by means of information technology.
- Cyber meddling violates
  1. the requirement to respect sovereignty,
  2. Constitutes an intervention into internal affairs of another State,
  3. and, when the cyber operations are not attributable to the State from which they were launched, breach of the due diligence obligation that requires States to ensure cyber operations with serious adverse consequences are not mounted from their territory.
- The term “cyber meddling” is often used to describe the external dimension of the broader concept of “information confrontation”.
- Information confrontation, in turn, depicts (mainly Russian) efforts to "to control its domestic populace and influence adversary states“ by “Informational-technical" and “informational-psychological" means. The former encompasses network operations relating to defense, attack, and exploitation with the latter relating to "attempts to change people's behavior or beliefs in favor of Russian governmental objectives means.

Cyber meddling: recent examples

1. April 2007 Estonia was targeted by a series of (Russian-based) cyberattacks on financial, media, and government websites.
2. In July 2008, the website of the Georgian president, Mikheil Saakashvili, was rendered inoperable for twenty-four hours by a series of denial of service attacks.
3. In mid-January 2009, Kyrgyzstan's two main Internet-Service Providers came under a large-scale DDoS attack, shutting down websites and e-mail within the country, effectively taking the nation offline. The attacks came at a time when the country's president, K. Bakiyev, was being pressured by both domestic actors and Russia to close a U.S. air base in Kyrgyzstan
4. In 2015, the French broadcasting service TV5Monde was attacked by jihadist hackers who used malicious software to attack and destroy the network's systems and take all twelve of its channels off the air.
5. In 2015, a high-ranking security official stated that it was "highly plausible" that a cyber theft of files from the German Parliamentary Committee investigating the NSA spying scandal, was conducted by Russian hackers.
6. In December 2015 a cyber attack caused a power outage in Ukraine which left more than 200,000 people temporarily without power.
7. In May 2017, just before the French presidential election, more than 20,000 e-mails belonging to the campaign of Emmanuel Macron were uploaded on an anonymous file-sharing website.
8. In April 2017, the British House of Commons issued a report stating, in regard to the June 2016 collapse of the government's voter registration website less than two hours prior to the originally scheduled registration deadline (which was then extended), that "the crash had indications of being a DDOS 'attack.'"
9. In early 2017 a report by the ODNI asserted that the Russian government had interfered in the 2016 U.S. presidential election in order to increase political instability in the United States and to damage Hillary Clinton's presidential campaign by bolstering the candidacies of Donald Trump, Bernie Sanders and Jill Stein.
10. In late September 2018, there occurred credible evidence that Russian actors used disinformation campaigns in social networks to depress voter turnout in Macedonian referendum on the name change of the country, deemed essential for further EU and NATO integration.

How Cyber meddling is done?

- **Hacking** generally refers to unauthorized intrusion into a computer or a network.
- **Phishing** is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.
- **Propaganda** is the spreading of ideas, information, or rumor for the purpose of helping or injuring an institution, a cause, or a person.
- **Using fraudulent social media** accounts to pose as regular members or to organize political events (demonstrations).

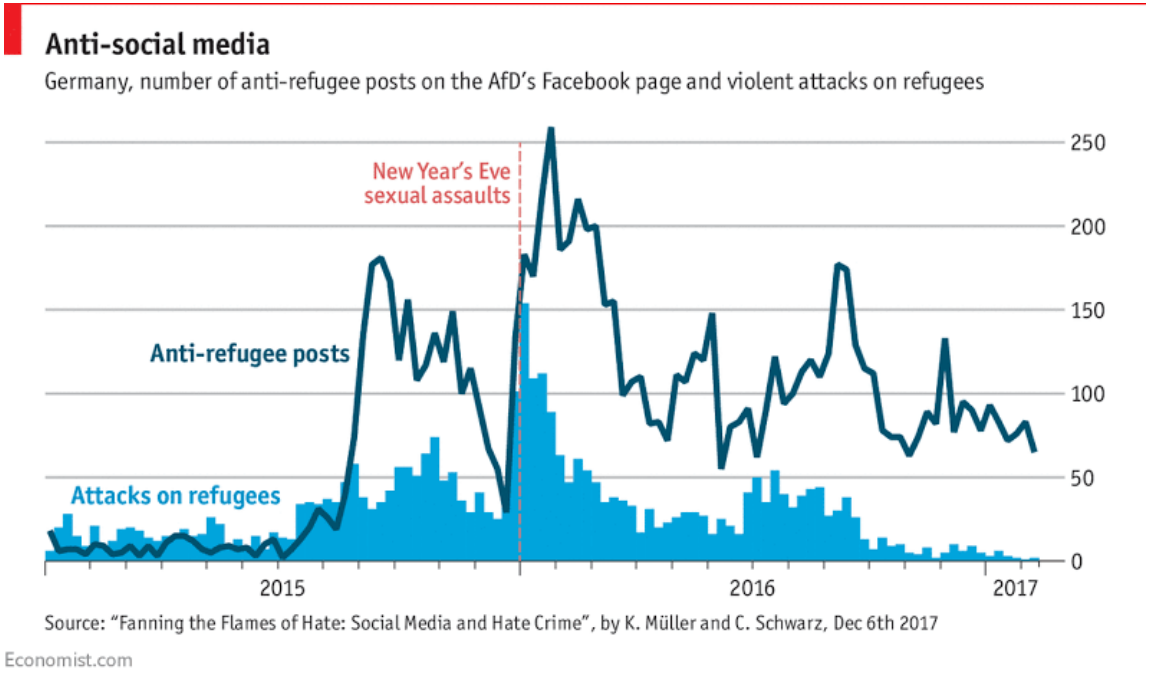


Strategies to prevent „virtual disenfranchisement

1. Consider electoral systems as part of critical infrastructure, institutionalize preparations to protect election processes, and broaden activities to the subnational levels.
2. *Focus on resilience measures: conduct regular vulnerability analyses and developing contingency plans. Legal measures should be explored through an inclusive process.*
3. Issue public statements to deter threat actors and educate voters about disinformation campaigns.
4. Train and educate political parties and campaigns to better protect against potential interference.
5. Conduct government-media dialogue, encourage media to take voluntary protective measures, and engage social media companies in mitigating potential threats.
6. Support international cooperation, particularly the sharing of lessons learned and best practices.

Müller/Schwarz 2018: Fanning the Flames of Hate: Social Media and Hate Crime

- The studies shows that right-wing anti-refugee sentiment on Facebook predicts violent crimes against refugees in municipalities with higher social media usage. To establish causality, we exploit exogenous variation in major internet and Facebook outages, which fully undo the correlation between social media and hate crime. Our results suggest that social media can act as a propagation mechanism between online hate speech and real-life violent crime.



Set combines data from 12 different sources: (1) Municipality-level data on anti-refugee hate crimes; (2) facebook data on posts, likes, and comments from the AfD pages; (3) hand-collected municipality-level data on Facebook user locations; (4) municipality-level data on internet outages; (5) a hand-coded dataset on major weekly Facebook outages; (6) socioeconomic data on the municipality and county level from the German Statistical Office; (7) election district voting data; (8) county-level data on broadband access; (9) survey data on internet usage from Eurostat; (10) municipality-level data on newspaper sales; (11) city-level data on neo-Nazi murders and historical anti-Semitism; and (12) weekly Google search data on major news events in our sample. The final panel dataset covers 4,466 German municipalities for the 111 weeks from 1st January 2015 to 13th February 2017

The German Network Enforcement Act, October 1, 2017 („NetzDG“)

- **Purpose:** The act seeks “to improve enforcement of the law in social networks”, and aims at combating fake news and hate speech. Regulatory offences may be fined by up to EUR 5 million for individuals and up to EUR 50 million for the platform provider itself.
- **Who?** “Act shall apply to telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public (social networks)” with more than 2 million registered users in Germany, regardless of where the social network is established.
- **What?** “Unlawful” content is content that is shared on social media with other users or in other ways made available to the public which unlawfully opposes the provisions of the Sections of the German Criminal Code that are listed in Sec. 1(3) NetzDG. The listed provisions deal with offences against the democratic constitutional state, the public order, the personal honour and the sexual self-determination.
- **How?** The procedure shall be easily recognisable, directly accessible and permanently available to users for submitting complaints. The procedure shall ensure that the social network provider takes immediate note of a complaint and checks whether the content in question is unlawful and subject to removal or blocking. The content must be deleted or blocked within 24 hours if it is manifestly unlawful. Other unlawful content has to be deleted or blocked “immediately”, meaning within a seven-day time limit during which the content is “evaluated”. This obligation does not apply to complaints lodged through means other than the complaint-management procedure. Very likely, geo-blocking would not suffice.
- **How often?** Social network providers which receive more than 100 complaints on unlawful content per calendar year are obliged to produce half-yearly reports on the handling of complaints about unlawful content on their platforms in German language.

Conclusion

1. Cyber security is an important topic for the diplomatic service of a country because it spans over the border of domestic and international politics.
2. Cyber security between states, thus far, has involved a limited level of violence, the reason for which les in the self-deterring nature of a possible adversarial response.
3. In contrast, online hate speech may be more pronounced because algorithms that determine the users newsfeed promote content that will maximize user engagement. It follows that posts that tap into negative, primal emotions like anger or fear, perform best in social networks and so proliferate. Anti-refugee sentiment, which combines fear of social change with us-vs.-them rallying cries, drive the discourse and ultimately the offline actions of social media users.

Sources

- Bendiek, Annegret 2016: Sorgfaltsverantwortung im Cyberraum. Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, Berlin: SWP.
- Erskine, Toni 2003. Making Sense of Responsibility in International Relations: Key Questions and Concepts, in: Erskine, Toni (ed.). Can Institutions Have Responsibilities? Collective Moral Agency and International Relations, Basingstoke: Palgrave MacMillan, 1-18.
- Geers, Kenneth, et al. 2014. World War C: Understanding nation-state motives behind today's advanced cyber attacks, FireEye, Milpitas, CA, USA, Technical Report.
- Heidbrink, Ludger 2016. Definitionen und Voraussetzungen der Verantwortung, in: Heidbrink, Ludger et al. (ed.). Handbuch Verantwortung, Wiesbaden: Springer VS.
- International Law Commission/ILC 2001. Responsibility of States for Internationally Wrongful Acts, in: Yearbook of the International Law Commission, 2001, Vol. II, Part Two, 26-143.
- Katzenstein, Peter J. (ed.) 1996. The culture of national security: Norms and identity in world politics, New York: Columbia University Press.
- Maurer, Tim 2011. Cyber Norm Emergence at the United Nations. An Analysis of the Activities at the UN Regarding Cyber-Security, in: Belfer Center for Science and International Affairs, Discussion Paper 11, https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf, [15.03.2018].
- Schmitt, Michael N. (ed.) 2017. Tallinn Manual 2.0 on the international law applicable to cyber operations, Cambridge: Cambridge University Press.
- Segal, Adam 2017. Chinese Cyber Diplomacy in a New Era of Uncertainty, Hoover Working Group on National security, Technology, and Law, Aegis Paper Series No. 1703, 2. Juni 2017, http://lawfareblog.com/chinese-cyber-diplomacy-new-era-uncertainty, [14.03.2018].
- **Steiger, Stefan, et al. 2018. Conceptualising conflicts in cyberspace, in: Journal of Cyber Policy, 1-19.**
- Valeriano, Brandon/Maness, Ryan C. 2014. The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11. in: Journal of Peace Research 51: 3, 347–360, doi:10.1177/0022343313518940.
- White House 2011. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World, Washington, DC, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, [16.03.2018].

Sources

- Hong, Mathias: *Das NetzDG und die Vermutung für die Freiheit der Rede, VerfBlog,* 2018/1/09, https://verfassungsblog.de/das-netzdg-und-die-vermutung-fuer-die-freiheit-der-rede/, DOI: https://dx.doi.org/10.17176/20180109-111851.
- Karl-Heinz Ladeur/Tobias Gostomzyk, Gutachten zur Verfassungsmäßigkeit des Entwurfs eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) i.d.F. vom 16. Mai 2017 – BT-Drs. 18/12356, erstattet auf Ansuchen des Bitkom, Mai 2017.
- Müller, Karsten and Schwarz, Carlo, Fanning the Flames of Hate: Social Media and Hate Crime (May 21, 2018). Available at SSRN: https://ssrn.com/abstract=3082972 or http://dx.doi.org/10.2139/ssrn.3082972
- Amanda Taub/Max Fisher 2018. Facebook Fueled Anti-Refugee Attacks in Germany, New research Suggests, in: New York Times, August 21, 2018, https://www.nytimes.com/2018/08/21/world/europe/facebook-refugee-attacks-germany.html

Norm Cycle-Model: Finnemore/Sikkink 1999