Digital Geopolitics: A Review of the Current State

Gazmend Huskaj
Geneva Centre for Security Policy, Geneva, Switzerland

g.huskaj@gcsp.ch

Abstract: The purpose of this research product is to present the current state of digital geopolitics. Digital Geopolitics is attracting much attention. It features in national digital strategies (for those countries that have those), and there is some research on the topic. However, until now, no systematic and up-to-date review of the scientific literature on digital geopolitics exists. This article reviews the scientific literature using the computational literature review method. 124 articles were identified in a scientific database. After removing articles without author and abstract, 120 articles remained to read, cluster and present in this research product. The findings present that research output increases from 2015 and onwards, 53 topics are covered in the data set, and top cited articles and top publication venues are presented. The answer to the research question is that based on the results and the manual clustering of topics, it is indicative that the Technology, Informational, Geography are Security areas have a high focus, with less focus on, for example, political and health areas.

Keywords: current; state; digital; geopolitics; review

1. Introduction - Why do we have to talk about Digital Geopolitics?

This article reviews the question what the current state of digital geopolitics is. Why is there a need to discuss Digital Geopolitics? There is no technology that has transformed societies in the ways that information- and telecommunications technology (ITC) has. The increased pace of digitalisation has opened opportunities to conduct e-commerce, e-governance, streamline processes, but also transformed intelligence, surveillance, reconnaissance, and command and control of joint military operations. The increased interconnectedness has also shortened the gap: threat actors can conduct successful attacks from their own territory, posing a threat to political stability, military secrets, and economic and social well-being. Cases such as the ransomware attacks on the private actors Colonial pipeline and Kaseya, and cyber espionage attacks on English-speaking organisations, dubbed APT1 (Hyvärinen, 2017), highlight how attacks like these can impact political, economic, social, and international stability.

Geopolitics is the "analysis of geographic influences on power relationships in international relations" (Deudney, 2013). The Swedish political scientist, Rudolf Kjellén, coined the term by the end of the 19th century or the beginning of the 20th century (Deudney, 2013). Kjellén argued that geopolitics is about "the problems and conditions within a state that arise from its geographic features" (Albert, 2022). Discussions on the political effects of geography on state security is nothing new. They range from Aristotle (384-322 BC), to Mackinder (1861-1947) (Deudney, 2013). Examples include climate, topography, and by the end of the 19th century, and beginning of the 20th century, the impact of new technologies on world politics. First, it was argued that control of the seas was important due to trade and transportation, that is, sea power. Then, when new technological advances led to railroads, new arguments were made that trade and transportation was now faster than sea routes, why land power was more important than sea power. With the discovery of the aeroplane, trade, transportation, and ways of waging war were different. Now, some geopoliticians and generals, like Giulio Douhet, argued that air superiority and air power theory was more advantageous than sea and land (Deudney, 2013). In summary, geopoliticians tried to understand how new technologies and related capabilities, during their interaction "with the largest-scale geographic features of the Earth would shape the character, number, and location of viable security units in the emerging global international system" (Deudney, 2013).

Digital, an adjective, is from the mid 15th century, "pertaining to numbers below ten" (Online Etymology Dictionary [OED], (n.d.)), from Latin digitus "finger or toe", where the "numerical sense is because numerals under 10 were counted on fingers" (OED, n.d.). During the development of the computer, digital could mean "using numerical digits" (from 1938); computers running on data in the form of digits (from 1945), and "in reference to recording or broadcasting, from 1960" (OED, n.d.). Digital, thus, is about using computers to compute data in the form of digits (often ones and zeroes). Today, in addition to digital, digitisation, digitalisation and digital transformation exist. According to Bloomberg (2018), digitisation "refers to taking analog information and encoding it into zeroes and ones so that computers can store, process, and transmit such information" (Bloomberg, 2018). Digitalisation however is not equally straightforward because many different definitions exist. One is about "the way in which many domains of social life are restructured around digital communication and media infrastructures" (Brennen & Kreiss, as cited by Bloomberg, 2018). Another states that digitalisation "is the use of digital technologies to change a business model and provide new revenue and value-producing

opportunities" (Gartner, as cited by Bloomberg, 2018). A third states that "digitalisation is the process of employing digital technologies and information to transform business operations" (Gartner, as cited by Muro et al. (2017), as cited by Bloomberg, 2018). In summary, digitalisation is the use of information systems (computers) and information- and telecommunication systems (ICT) to not only restructure societies, but also to restructure business operations. Thus, digital transformation is about the transformation of key business operations that affect products, processes, organisational structures, and management concepts, with the purpose of exploiting the benefits of digital technologies (Matt, Hess & Benlian, 2015).

In this research product, Digital Geopolitics is defined as the analysis of information systems (computers that create, process, store, retrieve and disseminate information, [Huskaj, 2019]) interconnected in networks of networks to build a large, global network (Cyberspace [Huskaj, 2019]), that together with the geographic features of Earth and space impact world politics, the military, economic, social, informational and infrastructure (PMESII) systems and subsystems. This is also why it is important to discuss digital geopolitics: cyberspace is ubiquitous and affects all domains of human life. Dunnett et al. (2017) provide discussions on the geographies of outer space.

2. Methods and Materials

Systematic literature reviews fulfil the criteria of "objectivity" and "repeatability". The computational literature review (CLR) method uses topic modelling based on the latent Dirichlet allocation algorithm (Blei et al., 2003). Additional algorithms were used in this research product, these are presented further down.

The source for collecting research products on digital geopolitics was Scopus. The Scopus® database is, 'the largest abstract and citation database of peer-reviewed literature' (Elsevier 2018). Scopus is a database that contains curated research information in a specific format. This makes it ideal to download and process the information computationally. On June 17, 2022, the keywords digital geopolitics were used in article title, abstract and keywords. The database presented 124 document results, from 1999 to 2022, published in 104 publication venues. The documents were cleaned to remove documents without author, abstract, or doubles, leaving 120 articles for review.

A first review of the 120 articles using the CLR-method revealed few insights and the decision to make a granular review of a subset of the dataset between 2015 to 2022 was taken. The 99 documents were cleaned by removing articles without author(s) and abstract, leaving 96 articles for review. The dataset presents an increase of research products per year, as Figure 1 and Figure 2 presents.

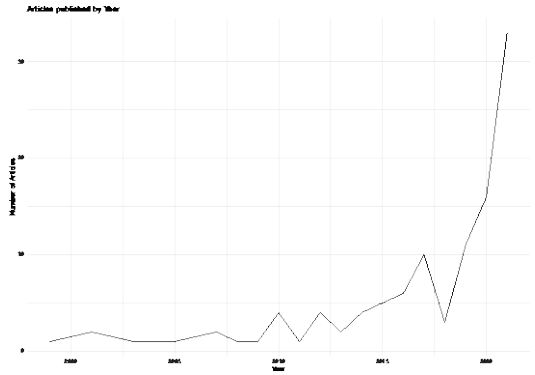

Figure 1: Research products published per year from 1999 to 2021.

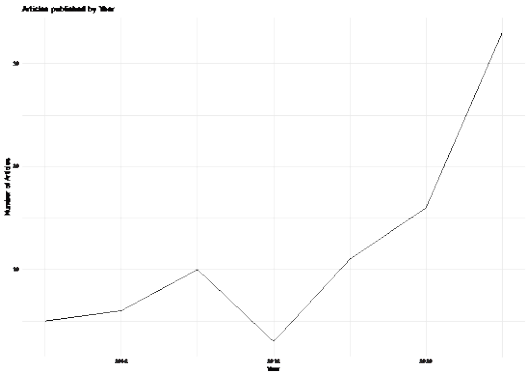

Figure 2: Research products published per year from 2015 to 2021.

Two additional algorithms were used in this research product. The ldatuning-algorithm (Nikita, 2016), and a modified algorithm inspired by the correlated topic model-algorithm (Blei & Lafferty, 2007) used by Roberts, Stewart, Tingley, and Airoldi (2013). The correlated topic model (stm) also includes information about trends over time, which makes it possible to discern how the interest in the different identified topics change over time. The keen reader will most likely ask the question how do you know how many topics reside in a dataset? Previously, researchers had to pre-set a value for the number of topics in a dataset and iterate the process until the results provided a set of topics which seemed reasonable. The topic-values were previously set to 30, 60, 90, or 120. However, today, the ldatuning-algorithm supports the research analyst in the relevant topics in a

dataset, also known as the k-value. Figure 3 presents the relevant topics, the k-value, for the dataset on digital geopolitics from 2015 to 2022.

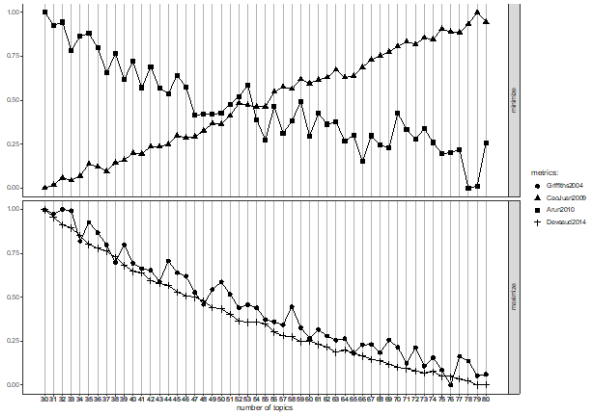

Figure 3: The ldatuning-algorithm to identify the number of topics in the dataset. The x-axis depicts no. of topics, the y-axis depicts algorithm-metrics.

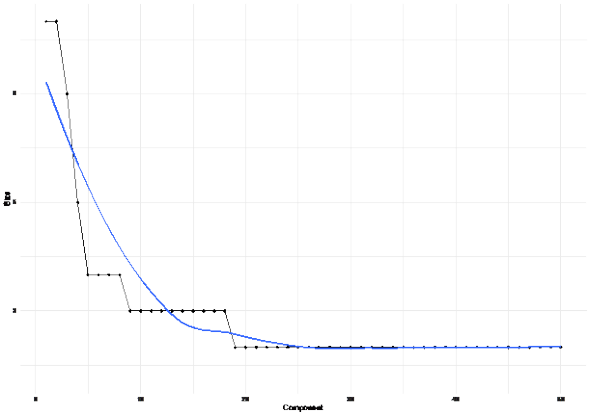

Figure 4: Presenting the 50 first co-author networks, where the top three consist of 11 co-authors, 11 co-authors, and 9 co-authors.

The results of the ldatuning-algorithm present that 53 topics exist in the dataset. Both algorithms, the LDA and the CTM, may be used to present each topic in word clouds. Word clouds is a method to visually present text. They present differences, similarities, and which words are most likely in a topic. The colours show different categories, and the size of the font presents the likelihood of which words will occur. An example of a word cloud is presented in Figure 4. It is up to the research analyst to infer the word clouds and provide a relevant label for the topic they discuss.

Finally, each topic consists of a set of research documents. These documents are, through the application of the LDA or CTM, statistically clustered into topics. Therefore, each topic, labelled by the research analyst, can be further analysed to present which research documents exist within that topic. Table 3 presents the insights provided by the 53 topics.

Figure 5: Topic 6 discusses geopolitical risk.

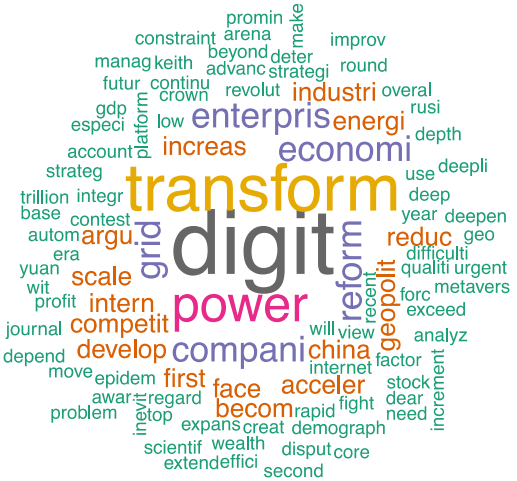

Figure 6: Topic 10 (the right) discusses digital transformation.

Finally, to cover some additional areas, the following five questions were used:

How does Digital Geopolitics relate to PMESII?; What factors can impact the geopolitical order and balance of power?; How is digital geopolitics important for the future of the Internet?

3. Results

The topic modelling presents 53 topics in the dataset. The topics are evaluated by the word clouds. The word clouds, topics, and papers, are presented in the supplementary material. Table 1 presents the most cited articles, while Table 2 presents the publication venues. The co-author of the authors is presented in Figure 5. Finally, as mentioned above, Table 3 presents the qualitative analysis of the 53 topics, manually inferred and labelled by the research analyst. Figures 6 to 8 present trends over time.

Table 1: Top 5 articles ranked by citation count.

No.	Authors	Title	Year	Source	Cites
1	Aouragh M., Chakravartty P.	Infrastructures of empire: towards a critical geopolitics of media and information studies	2016	Media, Culture and Society	44
2	Yang S., Yu X., Ding J., Zhang F., Wang F., Ma Y.	A review of water issues research in Central Asia	2017	Dili Xuebao/Acta Geographica Sinica	23
3	Peckham R., Sinha R.	Satellites and the New War on Infection: Tracking Ebola in West Africa	2017	Geoforum	18
4	Lavin M., Yang L., Zhao J.J.	Boys' love, cosplay, and androgynous idols: Queer fan cultures in mainland China, Hong Kong, and Taiwan	2017	Boys' Love, Cosplay, and Androgynous Idols: Queer Fan Cultures in Mainland China, Hong Kong, and Taiwan	17
5	Ermoshina K., Musiani F.	Migrating servers, elusive users: Reconfigurations of the Russian internet in the post-snowden era	2017	Media and Communication	15

Table 2: Top 5 publication venues ranked by number of articles and citation count.

Rank	Venue	Articles	Rank	Venue	Cites
1	Geopolitics	4	1	Media, Culture and Society	51
2	Media, Culture and Society	2	2	Dili Xuebao/Acta Geographica Sinica	23
3	Geoforum	2	3	Geoforum	22
4	Internet Policy Review	2	4	Geopolitics	16
5	Environment and Planning D: Society and Space	2	5	Media and Communication	15

Table 3: The 53 topics identified by the algorithm.

Topic no.	Insights
1. Natural Gas	Discusses natural gas supplies in China and related consumption (1.1).
2. Digitalisation and the Internet	Discusses digital diplomacy (2.1), disinformation (2.2) and the impact of technology (2.3).
3. Internet Geopolitics	Impacts on Indian cyber security (3.1), digital challenges (3.2), Internet Diplomacy (3.3).
4. Insecurity	Insecurity and security in young people (4.2) and implications for trade (4.1).
5. Definitions and Communities	Definitions on cyberwar (5.2) and social media's impact on community development (5.1).
6. Geopolitical Risk	Geopolitics and technological risks (6.1, 6.2).
7. The three seas initiative	A model for regional cooperation in central Europe (7.1).
8. Different digital discourse and tactics	Discourse analysis on the Internet (8.1) and tactics to be elusive (8.2).
9. Games for geopolitics	Visual novels (9.1), strategy games for education (9.2), and games for geopolitics (9.3).
10. Digital transformation	Digital transformation to empower power grids (10.1), and how digital transformation is impacting on power in geopolitics (10.2).

Topic no.	Insights
11. Digital war	The U.S.-China tech war (11.3), technology and infrastructure (11.2), and cultural geopolitics (11.1).
12. Geopolitics of travel blogging	Geopolitics and travel blogging (12.1).
13. Game layers	Game images and tech obsolescence (13.1).
14. Digital economies	Digital capacity of Russian tourist territories (14.1), and China in international digital economy governance (15.1).
15. Transition to the Cybersphere	China's transition to the cybersphere and its temporal-spatial governance (15.1).
16. Geographical places	Mediated geographies (16.1) and exploring the semantic and geographic space of Catalonia (16.2).
17. The arctic	The arctic and future opportunities in logistics (17.1).
18. Undersea Cables	The security politics of undersea cables (18.1).
19. European Energy Imports	European Energy import demands (19.1).
20. Geopolitics and digital power competition	The geopolitics of social media platforms (e.g. TikTok) (20.1), the impact of geotechnics (automation, machines) on geopolitics (20.2), Geopolitics, jurisdiction and surveillance (20.3).
21. Chinese interests	Tech-geopolitics (US-China trade war) (21.1), and Huawei's expansion (21.2).
22. Digital mapping	Using digital maps in disputes (22.1), mapping North Korea (22.2), and the Geographies of digital culture (22.3).
23. Cybersecurity	Cybersecurity development in the context of digital transformation (23.1), and the EU's response to cyber threats (23.2).
24. Digital geopolitics	Digital geopolitics of grime (24.1), and geopolitics and digital representations of space (24.2).
25. Data colonialism	Decolonising data colonialism (25.1).
26. Employment and platforms	Platforms of work, labour and employment (26.1), and digital relationships (26.2).
27. Education	A "Covid Collective" - the Philosophy of education (27.1).
28. Digital performance	Online performance (28.1) and the digital humor of the baltic Russian-speaking social media users (28.2).
29. States and algorithms	Cyberspace is ungoverned (29.1) and proactive state geographies (29.2).
30. Maps and claims	The role of maps in territorial disputes (30.1).
31. Data infrastructure	The Schengen Information System (31.1).
32. Fan cultures	Queer fan cultures in China, Hong Kong and Taiwan (32.1), and dismantling authoritarianism in Asia through digital means (32.2).
33. Foreign interference	Attacking democracy through digital means (33.1).
34. Unidentified	IP, piracy and counterfeiting (34.1).
35. Freedom of Expression	Freedom of expression in digital transition (35.1).
36. Education and humanoid robots	Humanoids in digital health education (36.1).
37. Connectivity and economic growth	Alternatives to connectivity (37.1), economic growth, and war on terror (37.1).
38. Dissent	Conflict and visual politics (38.1), and dissent in the digital age (38.2).
39. Humans, States and Satellites	Human rights through visual culture (39.1), state power and technology in India (39.2), satellite-based activism (39.3) and satellites to track Ebola (39.4).
40. Soft Power	Soft power and diplomacy in the pacific (40.1).
41. Vaccination Themes	The Sputnik vaccine (41.1) and digital vaccine certification (41.2).
42. Platforms	The globalisation of TikTok (42.1) and countering platform finance (42.2).
43. Processes	Commodification processes in relation to knowledge and publishing in journals (43.1) and triunity in the process of formation (43.2).

Topic no.	Insights
44. Migrant caravan	The digital life of #migrantcaravan and Twitter as a spatial technology (44.1), and aspects within the gulag architectonic (44.2).
45. Big data	The role of big geospatial data in the Covid-19-pandemic (45.1), big data and ethical challenges (45.2), and a cross-disciplinary exploration on AI-literacy (45.3).
46. Global internet	Traffic analysis in Cyberspace (46.1) and Chinese thoughts on cyber sovereignty (46.2).
47. Water in Central Asia	Water issues in Central Asia (47.1).
48. Digital development	The three seas initiative, geopolitics, economics and infrastructure (48.1, 48.2), and Russia's geodigital interests (48.3).
49. Business relationships	Australian-European economic and geopolitical relationships (49.1).
50. Copper logistics	Logistics along the line of copper (50.1).
51. Global digital currency	Digital currency (stable coin) as a reserve asset (51.1) and digital communication disrupting hegemonic power (51.2).
52. Digital storytelling	Digital storytelling (52.1, 52.3), and the geopolitics of Digital Space (52.2).
53. Digital platforms	China's stance against tech monopolies (53.1).

Manual clustering the topics reveals the following areas as depicted in Table 4.

Table 4: Manual clustering of topics into the different areas. NOTE: each number represents the topic number as depicted in Table 3.

Domain	Sub-topic	Domain (cont.)	Sub-topic (cont.)
Political	40	Energy	1, 19
Military	5, 11	Technology	2, 3, 10, 13, 15, 20, 24, 25, 28, 29, 31, 39, 42, 48, 51, 53
Economic	14, 37, 49	Education	37, 36
Social	9, 26, 32, 44	Health	41
Informational	8, 12, 22, 35, 38, 43, 45, 52	Security	4, 6, 23, 33, 47
Infrastructure	7, 46, 50	Unidentified	34
Geography	16, 17, 18, 21, 30		

In the introduction, the case for why digital geopolitics is important to discuss was made: cyberspace is ubiquitous, affects all domains of human life, and supporting PMESII-systems. This section will present how digital geopolitics relates to PMESII.

3.1 How does digital geopolitics relate to PMESII?

The ransomware attack, by the Russian-based DarkSide, on Colonial pipeline, the largest fuel pipeline in the U.S., had a great impact on the daily lives of Americans (Turton & Mehrotra, 2021). First, because the attackers encrypted the information systems of Colonial, the company was unable to operate the pipeline. Colonial decided to turn off the pipeline, the first time since it was turned on in 1964 (Turton & Mehrotra, 2021). The cyber security firm Mandiant was called in to investigate the attack (Kerner, 2022). While the pipeline was turned off, gas stations were unable to receive the standard amount of gas, which led to some gas stations running out. There were also reports that this could hit the aviation industry. The impact on the ground was long queues of Americans to buy gas, where the price of gas rose to $3.05 per gallon (~ 4.55 litres) (Dean, 2021). The U.S. government deemed the ransomware attack a national security threat and the President declared a state of emergency (Kerner, 2022). Management paid the $4.4 million ransom (Turton & Mehrotra, 2021). The FBI was able to follow the trace of bitcoin and recovered around $2.4 million after the Department of Justice "got a court order to seize the bitcoin" (Kerner, 2022). On June 16, at the Biden-Putin summit in Geneva, Switzerland, President Biden informs President Putin that some critical infrastructures should be "off-limits" (Soldatkin & Pamuk, 2021). Later, the partner of DarkSide, REvil, was targeted by the FBI, US Cyber Command (CYBERCOM), the Secret Service, and like-minded countries (Kellerman, as cited by Menn & Bing, 2021).

Analysing the case results in the following stakeholders involved: DarkSide and the target, Colonial Pipeline. Those impacted were suppliers of fuel and the citizen. The US President declared a state of emergency, the DoJ got a court order, the FBI recovered some of the ransom, and President Biden and President Putin met in Geneva.

Later, the FBI, US CYBERCOM, the Secret Service and like-minded countries were involved, dismantling REvil's infrastructure. From a PMESII-systems-perspective, the ransomware attack impacted world politics (President Biden and President Putin met in Geneva), CYBERCOM (military) conducted offensive cyberspace operations on REvil's infrastructure, the gas prices (economy) went up, long queues to gas stations developed (social), Colonial pipeline's information systems (information) were taken ransom, Colonial pipeline is critical infrastructure (infrastructure), finally, the attack was done by a Russian-based threat actor (geography). The remaining two cases, Kaseya and APT1, are left to the reader to analyse according to the case above.

3.2 So, what factors can impact the geopolitical order and balance of power?

As noted above, in Table 4, any impact on geographical, space, and PMESII-systems and subsystems can affect the geopolitical order and balance of power. One area that is overly presented is Technology. Advances in technology have, as mentioned in the introduction, shaped human life, societies and even the geopolitical order and balance of power. Topic 11 for example, discusses the U.S.-China Tech War, and Topic 21 discusses tech-geopolitics and Huawei's expansion. The U.S.-China tech war is a complicated topic. However, the Chinese companies Huawei and ZTE provide numerous technologies, where 5G telecommunications being one of them. 5G telecommunications equipment is needed to build the backbone of 5G networks. However, the U.S. intelligence community, and their counterparts in the U.K., Australia, Canada, and Sweden, to name a few, have voiced Chinese e-espionage-concerns of implementing 5G telecommunication equipment from Huawei or ZTE in the backbone infrastructure for 5G networks. The Chinese Communist Party (CCP) have accused the U.S. of protectionism. These back-and-forth accusations have led to what journalists call a "trade war".

Topic 2, 33, and 35, cover informational topics such as disinformation, foreign interference, and freedom of expression. Disinformation is extensively used by Chinese- and Russian-based threat actors, but also criminal entities. This has been especially evident during the Covid-19-pandemic, where Chinese-based threat actors have conducted cyber espionage on labs developing vaccines (BBC, 2020); Russian-based threat actors conducted cyber espionage on labs developing Covid-19-vaccines (NCSC, 2020). In addition, Covid-19-related disinformation campaigns from China, Iran, Russia and Tunisia providing false information have been identified and taken down by Google (Cimpanu, 2020). The combination of cyber espionage on labs developing Covid-19-vaccines and disinformation campaigns providing false Covid-19-information, lead to the Chinese and Russians accelerating their own Covid-19-vaccines at a cheaper cost (they're stealing the knowledge), at the same time, through disinformation campaigns erode trust between populations and their own governments, leading to phenomena as "anti-vaxxers".

In summary, as noted from the results presented in Table 3 (insights), and real-world cases, it is evident that factors like geography, space, and PMESII-systems, can impact the geopolitical order and balance of power.

3.3 Now, how is digital geopolitics important for the future of the Internet?

The analysis of internetworked information systems together with the geographic features of Earth and space are all important to monitor with the purpose of identifying threats, vulnerabilities, and related risks to the same. The purpose is to ensure that information that is created, processed, stored, retrieved and disseminated by information systems and humans, remains confidential, has its integrity untouched, and is available to those that have the right to access that information. It is evident that as technology has had huge positive transformational impacts on societies, the same can be misused by threat actors, ranging from states, state-sponsored threat actors, to organised crime groups and lone-wolf actors. Thus, as 5G-technologies are implemented, 6G-technology-seminars are held, to ensure that societies still thrive from these technologies, it is important that current and future leaders, professionals and technologists, work to ensure a safe, secure, and trustworthy Internet.

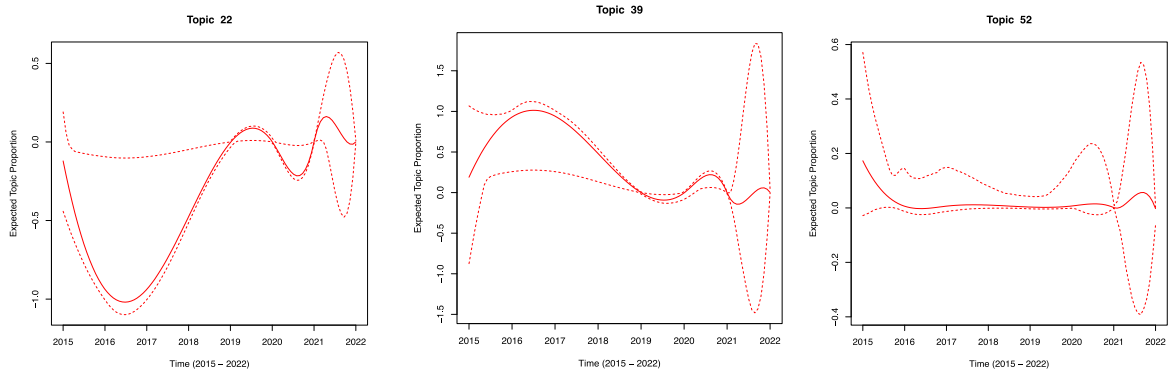

Figure 7: Trends on three topics from 2015 to 2022. Topic 22 – How digital maps are increasingly used in territorial disputes; Topic 39 – A declining trend about human rights through visual culture, state power and technology in India, and satellite-based activism; Topic 52 – How digital storytelling has shifted during the years.

4. Discussion

The answer to the question *what the current state of digital geopolitics is,* is that based on the results and the manual clustering of topics, it is indicative that the Technology, Informational, Geography are Security areas have a high focus, with less focus on, for example, political and health areas. Table 5 presents the biggest area-cluster in a descending order.

Table 5: The biggest domain-cluster in descending order.

Domain	Topics	Domain (cont.)	Topics (cont.)
Technology	16	Education	2
Informational	8	Energy	2
Geography	5	Military	2
Security	5	Health	1
Social	4	Political	1
Economic	3	Unidentified	1
Infrastructure	3		

The technology area consists of 16 topics. These topics are about algorithms, data, development, digitalisation, infrastructure, platforms, power issues, satellites, and transformation. It comes as no surprise that the technology area covers discussions on hardware, software, and telecommunications. This is essentially those fundamental technologies that have transformed societies from the Industrial Age to the Information Age. As computational power is increasing to process the vast amount of data that humans are creating, stored in data centres thanks to improved storage, transferred at speeds close to speed-of-light, with new advances on algorithms, machine-learning and "AI"-in general, humankind can really exploit the advantages these new technologies bring to improve human life. However, what is also evident is that the same technologies can be used for malicious purposes, but also to compete on how states should be governed (for example, democratic, autocratic), the world, different phenomena, and in essence, reality is perceived. Furthermore, these technologies are enabling ways to augment reality by visualising it, and interacting with it, in ways never possible before. The more of our senses that can be used to interact with these augmented realities, the more difficult it will be to discern "reality".

There are already challenges today where threat actors are conducting cyber-enabled disinformation operations targeting people and creating rifts in societies, but also rifts between societies and their elected. First, thanks to the ability to manipulate information in ways that it triggers people's worries', it is very easy to create these rifts, or to create doubt in an election system that the results are accurate, or if a vaccine is safe or not. As the ordinary citizen and user of these technologies can choose those who they want to interact with, it is very easy for them to choose the information that affirms/confirms those predetermined biases. Thus, threat actors are

directly and/or indirectly (through proxies) able to create informational "anti-access/area-denial spheres". Which leads to the Informational area.

The Informational area consists of 8 topics. The informational area is built on information that is visualised (e.g., maps), information created and shared by other humans, where they express their views on various topics, and related narratives. In essence, information within a given context framed from the perspectives of the beholder. Thanks to the technological areas above, humans are now able to exploit the benefits of new technological advancements, create content, tell stories, and reach audiences that pre-technological areas were not possible before. For example, in 2011, Pastor Terry Jones burned the Koran. Unconfirmed information states that the Afghanis were unaware of this case, until mainstream media began to report about it. Once the information ("news") reached Afghanistan, it led to massive violent protests where a mob attacked the UN camp in Mazar-e Sharif. Seven people were killed (Sief, 2011). What is maybe even somewhat ironic, is the title of the news article: "Florida pastor Terry Jones's Koran burning has far-reaching effect", which contains the words "far-reaching". Without these technologies, it is likely that the "Koran-burning"-information would have never reached the other side of the world, at the speed that it did, with the visual information that it did, resulting in the violent actions that it did.

The area of Geography consists of 5 topics. It consists of physical places (e.g., the Arctic and China), undersea places, and the role of geographical places in territorial disputes. The case for the arctic is quite self-explanatory. Climate change is having an impact on the arctic, melting the ice, leading to new opportunities to find resources and exploit those resources. This has led to a competition between various states, such as Canada, Russia and the U.S. China wants also to be a part of this and sees an opportunity. Therefore, geography, just like in the past, still can impact on world politics.

The Security area consists of 5 topics. It consists of lack of security, geopolitical risk, cybersecurity, attacks on democracy and water security. As noted, security, and the absence of security, is a broad topic. Cyber security, or the lack of it, can truly have an impact on world politics, and on international security, just like presented earlier. Therefore, cyber security, on all levels, and all domains, is important. The challenges are also many and range from identifying unintentional vulnerabilities in hardware and software, to the intentional search for vulnerabilities, to exploit them, and attack for espionage and/or criminal purposes. Other challenges that exist is public-private partnerships. The private sector owns much of the underlying infrastructure, and the private sector is responsible for the rapid development of technology and associated hardware and software. The public sector is not coping. Therefore, to ensure trust, certain measures need to be taken by both parties to ensure that sensitive information is shared securely and trust that the other party will not use it for their own advantages. In the U.K. for example, the National Cyber Security Centre (NCSC) has something known as "Industry 100". Industry 100 is "the principal initiative from the NCSC to facilitate close collaboration with the best and most diverse minds in UK industry" (NCSC, 2022). What is also noteworthy, is that "all i100 secondees will require a Security Check clearance" (NCSC, 2022).

The Security Check clearance is mandatory because it is likely that participants will have access to sensitive information which, if released publicly, could impact on British National Security. In the U.S., US Cyber Command has something known as "USCYBERCOM Industry Day 2022". This event gives USCYBERCOM the opportunity "to connect with private industry to communicate its capability requirements and challenges" (USCYBERCOM, 2022). Naturally, private industry partners are vetted before being accepted to the event.

What is the role of the private sector then? The private sector can also take their own initiatives. The Tech Accords, of which more than 100 companies have signed, has the mission to promote "a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats" (Cybersecurity Tech Accord, 2022). Brad Smith, President & Vice Chair at Microsoft, argued the need for a "Digital Geneva Convention" (Smith, 2017). The problem that led to this initiative was naturally cybercriminal attacks, state, and state-sponsored cyber attacks. Smith (2017) argued that private sector companies, including Microsoft, are doing as much as they can, but Governments should now step up to. While the initiative is good, there are those who would see this as an opportunity to remove the existing Geneva Conventions.

Finally, looking at the Russo-Ukraine war, the private sector has shown its ability to contribute to cyber defence: identifying destructive malicious software, especially in the Ukrainian Rails System. What would the consequences have been if the malicious code had "detonated", rendering trains unable to roll, making it impossible for civilians to flee?

Acknowledgements

The views and opinions are of the author and do not necessarily reflect those of the GCSP. Also, I would like to thank Dr. Richard Vidgen for his advice on the CLR and STM and to contact Dr. Michael J. Mortenson, who in turn shared his expertise on the CLR and the STM.

References

Albert, M. (2022). Rudolf Kjellén. Accessed 21 June 2022. Retrieved from https://www.britannica.com/biography/Rudolf-Kjellen.

BBC. (2020). US charges Chinese Covid-19 research 'cyber-spies'. Accessed 22 June 2022. Retrieved from https://www.bbc.com/news/world-us-canada-53493028.

Blei, D. M., & Lafferty, J. D. (2007). A correlated topic model of Science. The Annals of Applied Statistics, 17–35.

Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Dirichlet allocation. The Journal of Machine Learning Research, 3, 993–1022.

Cimpanu, C. (2020). Google said it took down ten influence operation campaigns in Q2 2020. Accessed 22 June 2022. Retrieved from https://www.zdnet.com/article/google-discloses-new-takedowns-of-influence-ops-on-its-sites/.

Cybersecurity Tech Accord. (2022). Mission Statement. Accessed 22 June 2022. Retrieved from https://cybertechaccord.org/about/.

Dean, G. (2021). Drivers face $3 gas prices after the Colonial Pipeline cyberattack, and some gas stations have run out completely. Accessed 21 June 2022. Retrieved from https://www.businessinsider.com/gas-prices-colonial-pipeline-cyberattack-fuel-east-coast-2021-5?r=US&IR=T.

Deudney, D.H. (2013). Geopolitics. Accessed 21 June 2022. Retrieved form https://www.britannica.com/topic/geopolitics.

Dunnett, O., Maclaren, A. S., Klinger, J., Lane, K. M. D., & Sage, D. (2019). Geographies of outer space: Progress and new opportunities. Progress in Human Geography, 43(2), 314–336. https://doi.org/10.1177/0309132517747727

Huskaj, G. (2019). The Current State of Research in Offensive Cyberspace Operations. In: Proceedings of the 18th European Conference on Cyber Warfare and Security, Academic Conferences and Publishing International Limited, 2019, p. 660-667.

Hyvärinen, N. (2017). APT1 - What happened next? Accessed 21 June 2022. Retrieved from https://blog.f-secure.com/apt1-what-happened-next/.

Kerner, S.M. (2022). Colonial Pipeline hack explained: Everything you need to know. Accessed 22 June 2022. Retrieved from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Matt, C., Hess, T. & Benlian, A. (2015). Digital Transformation Strategies. Bus Inf Syst Eng 57, 339–343 (2015). https://doi.org/10.1007/s12599-015-0401-5.

Menn, J. & Bing, C. (2021). EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline. Accessed 22 June 2022. Retrieved from https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

NCSC. (2020). Advisory: APT29 targets COVID-19 vaccine development. Accessed 22 June 2022. Retrieved from https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

NCSC. (2022). Industry 100. Accessed 22 June 2022. Retrieved from https://www.ncsc.gov.uk/section/industry-100/about.

Nikita, M. (2016). ldatuning. Retrieved from https://cran.r- project.org/web/packages/ldatuning/ldatuning.pdf

Online Etymology Dictionary. (n.d.). Digital (adj.). Online Etymology Dictionary. Accessed 21 June 2022. Retrieved from https://www.etymonline.com/word/digital#etymonline_v_31427.

Roberts, M. E., Stewart, B. M., Tingley, D., & Airoldi, E. M. (2013). The structural topic model and applied social science. Advances in Neural Information Processing Systems Workshop on Topic Models: Computation, Application, and Evaluation,

Sief, K. (2011). Florida pastor Terry Jones's Koran burning has far-reaching effect. Accessed 22 June 2022. Retrieved from https://www.washingtonpost.com/local/education/florida-pastor-terry-joness-koran-burning-has-far-reaching-effect/2011/04/02/AFpiFoQC_story.html.

Smith, B. (2017). The need for a Digital Geneva Convention. Accessed 22 June 2022. Retrieved from https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Soldatkin, V. & Pamuk, H. (2021). Biden tells Putin certain cyberattacks should be 'off-limits'. Accessed 22 June 2022. Retrieved from https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

Turton, W. & Mehrotra, K. (2021). Hackers Breached Colonial Pipeline Using Compromised Password. Accessed 21 June 2022. Retrieved from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

USCYBERCOM. (2022). USCYBERCOM Industry Day 2022. Accessed 22 June 2022. Retrieved from https://dreamport.tech/USCC-Industry-Day/.