METHODOLOGICAL NOTE

Cyber Conflict Portal

Introduction[1]

The Cyber Conflict Portal documents international and domestic incidences of cyber conflict. Conflictual and competitive international relations manifest in the use of information and communication technologies (ICTs) to engage in (a) cyber espionage, (b) effect-creating cyber operations, (c) low-intensity and high-frequency cyber campaigns, (d) cyber-enabled assaults against the international community, (e) domestic cyber conflict and cyber-enabled human-rights violations and (f) cybercrime associated with proxy actors. The first module of the Portal examines cyber conflict through the dynamics and elements of effect-creating cyber operations conducted by or against states. Effects are understood as changes in the targeted or directly affected system(s) (for instance, mere exfiltration would not be considered an effect-creating operation).

We focus on cyber conflict as the manifestation of international relations, where parties pursue mutually incommensurable demands in and through cyberspace, conducting deliberate and purposeful activities – cyber operations. Acknowledging that most cyber conflict manifests in previously adversarial relationships and centres on the use of ICTs, we nevertheless see value in examining and studying cyber conflict as a phenomenon – especially as the opportunity of conducting cyber operations may have introduced new developments into international contestation more broadly.

Our methodological assumption is that a thorough study of the facts and circumstances of individual cyber operations deepens our understanding of international relations playing out in and through cyberspace. With a vested interest in cyber conflict prevention, we claim that deeper understanding of the problem allows more informed consideration of possible and alternative political, normative and technical solutions. Our core ontology of cyber operations comprises data about the *attacker*, the *target*, the *act* and its *effect*. The wider, 'rim', ontology extends to associated features of a cyber operation – its *pretex*t and *implications*.

Our work builds on and draws from other datasets that focus on cyber operations and the use of ICTs in dyadic relationships. Compared to the work done by CSIS (Significant Cyber Incidents),[2] we focus more narrowly on cyber operations rather than incidents, and the economic impact of such operations is secondary to the fact that they are associated with a state actor as a target or as a recipient. We seek to

[1] This research has been supported by Microsoft NV (2019), the Tallinn University of Technology through the ICT Development Program of the Estonian Ministry of Economic Affairs and Communications (2018–2020) and the EU Cyber Direct project funded by the European Union.

[2] 'Significant Cyber Incidents,' Center for Strategic and International Studies, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

This project is funded by the European Union.

offer a thoroughly documented factual account of operations, thus complementing the work done by the CFR Cyber Operations Tracker.[3] Our research interests are closest to the work done by Maness, Valeriano and Jensen.[4] However, we expand our inquiry to operations that may not have a pre-defined dyadic context or that go beyond dyadic relationships between any two states. When developing our dataset, we have also drawn from the research of Mitchell and Pytlak.[5]

Codebook of effect-creating cyber operations

SHEET/ COLUMN	LOCATION[6]	PURPOSE	TYPOLOGY AND CONTENT
01A	DB	[CPI CODE]: internal enumeration	Consists of year and a chronological incident number.
01B	DB	[NAME]: identification, clarity and unique reference	We use the most common name there is and avoid entirely descriptive names. If the name derives from another name (e.g. Estonia, Georgia), we add the year of occurrence.
01C	DB	[ACCESS YEAR]: chronological, contextual and pattern analysis, for instance: character of the operation in terms of duration, chronology, links to other incidents (for instance, connected incidents to facilitate later operations).	Documents the first associated access to the system by year. Not applicable in case of incidents that do not require previous active presence in the affected system (denial of service attacks). Where the access year is not known to the public, this has been coded as 'unknown'.
01D	DB	[ACCESS MONTH]: chronological, contextual and pattern analysis, for instance: character of the operation in terms of duration, chronology, links to other incidents (for instance, connected incidents to facilitate later operations).	Documents the first associated access to the system by month. Not applicable in case of incidents that do not require previous active presence in the affected system (denial of service attacks). Where the access month is not known to the public, this has been coded as 'unknown'.
01E	DB	[ACCESS DAY]: chronological, contextual and pattern analysis, for instance: character of the operation in terms of duration, chronology, links to other incidents (for instance, connected incidents to facilitate later operations).	Documents the first associated access to the system by day. Not applicable in case of incidents that do not require previous active presence in the affected system (denial of service attacks). Where the access day is not known to the public, this has been coded as 'unknown'.

[3] 'Cyber Operations Tracker', Council on Foreign Relations, https://www.cfr.org/cyber-operations/.
[4] Ryan C. Maness, Brandon Valeriano and Benjamin Jensen, 'The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011,' Version 1.5, https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.
[5] George E. Mitchell and Allison Pytlak, 'Correlates of state-sponsored cyber conflict', in *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (London: Routledge, 2020), 22–35.
[6] DB = [database]; FS = [factsheet].

01F	DB	[START YEAR]: chronological, contextual and pattern analysis; character of the operation in terms of duration, chronology, context, coinciding events (holidays, political triggers).	Documents the first known effect on the system by year. Where the start year is not known to the public, this has been coded as 'unknown'.
01G	DB	[START MONTH]: chronological, contextual and pattern analysis; character of the operation in terms of duration, chronology, context, coinciding events (holidays, political triggers).	Documents the first known effect on the system by month. Where the start month is not known to the public, this has been coded as 'unknown'.
01H	DB	[START DAY]: chronological, contextual and pattern analysis; character of the operation in terms of duration, chronology, context, coinciding events (holidays, political triggers).	Documents the first known effect on the system by day. Where the start day is not known to the public, this has been coded as 'unknown'.
01I	DB	[END YEAR]: chronological, contextual and pattern analysis and characterise the operation in terms of duration, chronology; to assess temporal aspects of managing the incident.	Documents the known or reported termination of the effect on the targeted system (without covering possible economic and political repercussions) by year. Where the end year is not known to the public, this has been coded as 'unknown'.
01J	DB	[END MONTH]: chronological, contextual and pattern analysis; character of the operation in terms of duration, chronology; to assess temporal aspects of managing the incident.	Documents the known or reported termination of the effect on the targeted system (without covering possible economic and political repercussions) by year. Where the end month is not known to the public, this has been coded as 'unknown'.
01K	DB	[END DAY]: chronological, contextual and pattern analysis; character of the operation in terms of duration, chronology; to assess temporal aspects of managing the incident.	Documents the known or reported termination of the effect on the targeted system (without covering possible economic and political repercussions) by year. Where the end day is not known to the public, this has been coded as 'unknown'.
01L	DB	[FIRST REPORTED YEAR]: transparency (dark period before public awareness) and original points of reference (first reports) related to the operation.	Documents the first public indication of the incident by year. Where the year of initial public reference is not known to the public, this has been coded as 'unknown'.

O1M	DB	[FIRST REPORTED MONTH]: transparency (dark period before public awareness) and original points of reference (first reports) related to the operation.	Documents the first public indication of the incident by month. Where the month of initial public reference is not known to the public, this has been coded as 'unknown'.
01N	DB	[FIRST REPORTED DAY]: transparency (dark period before public awareness) and original points of reference (first reports) related to the operation.	Documents the first public indication of the incident by day. Where the day of initial public reference is not known to the public, this has been coded as 'unknown'.
02C	DB	[DYAD]: political contextualisation, causality and correlation research, reference	Dyad refers to the pre-existing adversarial relationship between jurisdictions or political entities involved in or affected by the operation.
O2D	DB	[ONGOING MILITARY CONFRONTATION]: causality and correlation research, e.g. linkage between use of ICTs and violent conflict, the nature and state of the dyad, possible escalation/de-escalation dynamics and the military use of ICTs/cyber means.	Military confrontation is active where frequent hostilities and destructive power are used between the rivals. 'Latent' refers to where escalation and the use of destructive (military) power is likely. 'Frozen conflict' means that the use of destructive power is settled by temporary, formal arrangement or de facto understanding. 'No' refers to where none of the above is occurring between parties in question.
02E	DB	[TYPE OF DISPUTE]: causality and correlation research, e.g. to determine trends and character of cyber conflict, pointing out links between dispute and ICTs opens strategies and possibilities of diplomatic and political prevention	Types of disputes are coded as ideological, territorial or economic, which refer to the primary reason or issue under dispute.
02F	DB	[GEOPOLITICAL SETTING]: causality and correlation research, implications and contextualisation.	Geopolitical setting is coded bilateral, regional balance of power or world order contestation, which refer to the primary geopolitical context of the conflict or the relationship of the parties to the conflict in question.
01	FS	[BACKGROUND]: broader contextualisation	The geopolitical, domestic and other events and circumstances that are associated with the operation.

05	FS	[TIMELINE]: chronological, contextual and pattern analysis; character of the operation in terms of duration and chronology.	Factual temporal aspects associated with the operation.
03C	DB	[ATTACK JURISDICTION I]: causality and correlation research, reference	Jurisdiction commonly associated with perpetrating or enabling the operation.
03D	DB	[ATTACK JURISDICTION II]: causality and correlation research, reference	Jurisdiction commonly associated with perpetrating or enabling the operation, filled only if applicable.
03E	DB	[ATTACK INVOLVED ENTITY]: causality and correlation research, e.g. potential allocation of responsibility to the entity or group implicated, operational organisation of cyber operations (e.g. mandates to be revised, activities to be regulated, capabilities, resources and doctrines to track).	State authority commonly associated with perpetrating or enabling the operation
03F	DB	[ATTACK INVOLVED PROXY]: causality and correlation research, e.g. associations between non-state entities/actors and states in cyber conflict.	Non-state authority/entity commonly associated with perpetrating or enabling the operation
03G	DB	[ATTACK INVOLVED INDIVIDUAL]: causality and correlation research, e.g. to understand the associations between individuals and states in cyber conflict.	Natural person commonly associated with perpetrating or enabling the operation (only if officially attributed)
03H	DB	[ATTACK NUCLEAR CAPABILITY]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	Possession of demonstrated nuclear explosive devices, derives from earlier research.
03I	DB	[ACCOUNTABILITY]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	The extent of citizens' political influence and freedoms, derives from earlier work of the World Bank.

03J	DB	[ATTACK FOREIGN DIRECT INVESMENT RANKING]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	Balance of payments of foreign direct investment and the international investment position, derives from earlier work of the IMF.
03K	DB	[GDP RANK]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	The nominal ranking of the jurisdiction primarily associated with the operation in terms of gross domestic product, derives from earlier work of the IMF.
03L	DB	[ATTACK GGE]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Participation in the UN GGEs.
03M	DB	[ATTACK OSCE]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Participation in the OSCE.
03N	DB	[ATTACK ASEAN]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the ASEAN.
03O	DB	[ATTACK OAS]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the OAS.
03P	DB	[ATTACK SCO]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the SCO.

03Q	DB	[ATTACK LAS]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the LAS.
03R	DB	[ATTACK G7]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the G7.
03S	DB	[ATTACK G20]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the G20.
03T	DB	[ATTACK CYBER COMMAND]: causality and correlation research, e.g. trends and patterns associated with cyber conflict.	Existence of cyber command in the time of operation.
04	FS	[ATTRIBUTION]: international relations associated with the operation. International policy and diplomacy analysis.	Facts about technical, political or legal attribution of the operation.
03U	DB	[TARGET JURISDICTION]: causality and correlation research, reference	Jurisdiction receiving or being primarily affected by the operation.
03V	DB	[TARGET JURISDICTION II]: causality and correlation research, reference	Jurisdiction receiving or being affected by the operation.
03W	DB	[TARGET ENTITY]: causality and correlation research, e.g. impact and response analysis.	State authority receiving or being affected by the operation.
03X	DB	[TARGET INTERNET INFRASTRUCTURE]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was electronic communications, domain name service or trust service provider).

03Y	DB	[TARGET GOVERNMENT]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a government entity).
03Z	DB	[TARGET COMMERCIAL]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a commercial entity).
03AA	DB	[TARGET STATE-OWNED]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a state-owned entity).
03AB	DB	[TARGET INDIVIDUAL]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a natural person).
03AC	DB	[TARGET CI SECTOR (I)]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a critical infrastructure entity).
03AD	DB	[TARGET CI SECTOR (II)]: causality and correlation research, e.g. detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a critical infrastructure entity).
03AE	DB	[TARGET CI SECTOR (III)]: detailed impact and response analysis.	If applicable (i.e. if the target or primary recipient was a critical infrastructure entity).
03AF	DB	[TARGET NUCLEAR CAPABILITY]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	Possession of demonstrated nuclear explosive devices.
03AG	DB	[TARGET ACCOUNTABILITY]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	The extent of citizens' political influence and freedoms, derives from earlier work of the World Bank.
03AH	DB	[TARGET GDP RANK]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	Derives from earlier work of the IMF.
03AI	DB	[TARGET FORIGN DIRECT INVESTMENT RANK]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	The nominal ranking of the jurisdiction primarily associated with the operation in terms of gross domestic product, derives from earlier work of the IMF.

03AJ	DB	[TARGET GGE]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Participation in the UN GGEs.
03AK	DB	[TARGET OSCE]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Participation in the OSCE.
03AL	DB	[TARGET ASEAN]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the ASEAN.
03AM	DB	[TARGET OAS]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the OAS.
03AN	DB	[TARGET SCO]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the SCO.
03AO	DB	[TARGET LAS]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the LAS.
03AP	DB	[TARGET G7]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the G7.

03AQ	DB	[TARGET G20]: causality and correlation research, e.g. the organisational dynamics between the parties to cyber conflict; international processes for prevention and remediation.	Membership of the G20.
03AR	DB	[TARGET COMMAND]: causality and correlation research, e.g. trends and patterns associated with cyber operations.	Existence of cyber command in the time of operation.
02	FS	[AFFECTED ENTITIES]: impact assessment.	Additional identifying information about the organisations, sectors or groups most affected by the operation.
04C	DB	[INITIAL ACCESS (MITRE ATT&CK FOR ENTERPRISE)]: causality and correlation research, e.g. priorities and strategies for technical, organisational and physical preventive measures.	Indicates Initial Access by techniques described in the MITRE ATT&CK for Enterprise. The entry vector is selected according to the most decisive technique for the initial foothold. Initial Access is not applicable for DDoS and DoS attacks.
04D	DB	[INITIAL ACCESS (MITRE ATT&CK FOR ICS)]: causality and correlation research, e.g. priorities and strategies for technical, organisational and physical preventive measures.	Indicates Initial Access by techniques described in the MITRE ATT&CK for ICS. The selection of the entry vector is done according to the most decisive technique for the initial foothold. This is applicable to cases where Industrial Control Systems were impacted.
04E	DB	[IMPACT (MITRE ATT&CK FOR ENTERPRISE)]: causality and correlation research, e.g. impact assessment and correlation between successful access and potential result.	Indicates impact of the operation by given categories of MITRE ATT&CK for Enterprise.
04F	DB	[ADDITIONAL IMPACT (MITRE ATT&CK FOR ENTERPRISE)]: causality and correlation research, e.g. impact assessment and correlation between successful access and potential result.	If applicable, indicates second impact under MITRE ATT&CK for Enterprise.
04G	DB	[IMPACT (MITRE ATT&CK FOR ICS)]: causality and correlation research, e.g. impact assessment and correlation between successful access and potential result.	Indicates the most severe impact of the operation described in MITRE ATT&CK for ICS.

06	FS	[TECHNICAL DETAILS]: priorities and strategies for technical, organisational and physical prevention and mitigation.	Factual assessment of technical, organisational and physical circumstances of the operation.
07	FS	[ENABLERS]: Prevention and mitigation analysis.	Facts-based analysis of the political and technical factors that conditioned the operation and/or contributed to its effect or implications.
05C	DB	[INFOSEC EFFECT]: causality and correlation research.	Classification of effect/impact under the CIA triad to promote and inform interdisciplinary analysis of cyber conflict. Loss of confidentiality means that data or information has been made accessible to unauthorised persons; loss of integrity refers to changes in data or information compared to their original purposes; loss of availability means data or information have been unavailable to intended or legitimate audiences.
05D	DB	[US MILITARY EFFECT]: causality and correlation research.	US military doctrinal classification of effect/impact under to draw attention to the correlation between military operational doctrine and actual effects and facilitate international dialogue focusing on the development and use of particular military capabilities. This classification comprises manipulation, denial (in the form of disruption and degradation) and destruction. Manipulation: JP 3-12 *Cyberspace Operations* (June 2018), p. II-7: Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in grey or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification and other similar techniques. It uses an adversary's information resources for friendly purposes, to create denial effects not immediately apparent in cyberspace. The targeted network may appear to operate normally until secondary or tertiary effects, including physical effects, reveal evidence of the logical first-order effect. Destruction: JP 3-12 *Cyberspace Operations* (June 2018), p. II-7: To completely and irreparably deny access to, or operation of, a target. Destruction maximises the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.

			Degradation: JP 3-12 *Cyberspace Operations* (June 2018), p. II-7: To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified. **Disruption**: JP 3-12 *Cyberspace Operations* (June 2018), p. II-7: To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100%.
05E	DB	[PHYSICAL EFFECT]: to understand the ratio of incidents that have had physical consequences and trends in the severity, orientation and sophistication of cyber-attacks over time, to direct preventive efforts.	Physical effect is coded where the operation caused damage to physical objects other than the computers or their components.
05F	DB	[CORPORATE DOWNTIME]: to understand the cost components of the incidents, assess the accuracy of the number and predict and minimise costs upon impact.	Known or alleged disruption caused in commercial services or production.
05G	DB	[ESTIMATED LOSS]: to understand the political reception and sensitivities the operation targeted or met and explain relevant responses and reactions.	Known or alleged monetary losses caused by the operation.
03	FS	[IMPACT AND SIGNIFICANCE]: implication and effect analysis.	
08	FS	[REMEDIES AND CONSEQUENCES]: response and remediation analysis.	Factual account of responses and remedies taken with regard to the operation.
09	FS	[PRIVATE SECTOR ENGAGEMENT]: response and remediation analysis.	Factual account of responses and remedies taken by private sector entities.
10	FS	[ADDITIONAL READING]: further analysis and references.	