SUPPLEMENTARY MATERIAL FOR ONLINE PUBLICATION

Appendix A: Comparison of Methodologies

Table 6. Comparison of Methodologies

Model	Advantages	Disadvantages	Fields of application
Input-output model	- Partial equilibrium (quantities only) and partial optimization[1] - No supply constraints - Clear distinction between direct and indirect impacts - Identification of supply chain linkages - Allows scenario modelling - Allows differentiation between sectors - Simplicity and transparency - Allows to measure ripple effects - Reliable data collection methodology - Allows to analyze the impact of inoperability in a particular sector	- Availability of reliable primary data - Does not capture inter-industry linkages changes over time - Assumption of constant returns on scale; fixed technical coefficients, infinite and perfectly elastic resources; infinite and perfectly elastic supply of resources; resources are efficiently used; linearity - No substitution between inputs to production processes - No mechanism for price adjustments - Inability to incorporate the reactions of economic agents to disasters[2] - Overestimation of indirect economic losses[3] - Determination of the impacts only in a short-term horizon[4]	- Natural catastrophes (e.g., Hallegatte, 2008) - Critical infrastructure systems (e.g., Lin et al., 2016) - Material use and emissions (e.g., Guevara and Domingos, 2017) - Energy price shocks, interest rates, and heat emissions (e.g., Berg et al., 2015) - Global production networks (e.g., Niknejad and Petrovic, 2016) - Waste management (e.g., Nakamura and Kondo, 2018) - Terrorism (e.g., Santos and Haimes, 2004)
Computable general equilibrium models	- General equilibrium (prices and quantities) and full optimization - Demand and supply - Captures sector interdependences due to its price-quantity interconnectedness - Behavior of economic agents are modelled explicitly through utility and profit maximizing assumptions - Promising if the shocks under consideration affect many countries and sectors concurrently - Allow for the possibility of input substitution - Non-linearity improves the representation of the	- Extensive data requirement - No differentiation between direct and indirect impacts - Based on the neoclassical concepts of optimization and rationality - Assumptions about the market structure (perfect competition); production function; maximization behavior of households; Armington assumption[5]; non-convexities in production; social welfare; absence of market failures - Results are sensitive to the applied elasticities - Insufficient empirical foundation of the theoretical framework - High mathematical complexity	- Natural gas price effects (e.g., Zhang et al., 2017) - Valuation of air pollution co-benefits (e.g., Bollen, 2015) - Corporate income tax reform proposals (e.g., Bhattarai et al., 2017) - Electricity system (e.g., Langarita et al., 2019) - Tourism contribution to poverty alleviation (e.g., Njoya and Seetaram, 2017) - Impact of disease vaccination strategies (e.g., Miller et al., 2018)

[1] (West, 1995).
[2] (Poledna et al., 2018).
[3] (Koks et al., 2015).
[4] (Koks et al., 2015).
[5] The Armington assumption states that products from different import sources, although similar, are imperfect substitutes (Armington, 1969).

	actual economic conditions (e.g. economies of scale) - Determination of the impacts in the short-, medium- and long-term horizon[15]	- Black-box critique: low transparency and inexplicit indication of the factors driving the results[6] - Underestimation of indirect economic losses[14]	
Econometric models	- Well-established set of criteria for model valuation[7] - Forecasting capabilities, statistical rigorousness, provision of stochastic estimates[8]	- Require consistent time-series data over a long period of time - Extrapolation of the past - Difficulty in distinguishing direct and indirect effects[9]	- Natural disasters (Sahin and Yavuz, 2015; Okon, 2018) - Impact on emigration due to natural disasters (Saldaña-Zorrilla and Sandberg, 2009)

[6] See Piermantini and Teh (2005).
[7] See Rose (2004).
[8] See Okuyama (2007)
[9] See Rose (2004).

Appendix B: Industry classification

Table 7. Sectors Included in the Input-Output Tables of the OECD (OECD, 2018)

Industry code	Industry name
D01T03	Agriculture, forestry and fishing
D05T06	Mining and extraction of energy producing products
D07T08	Mining and quarrying of non-energy producing products
D09	Mining support service activities
D10T12	Food products, beverages and tobacco
D13T15	Textiles, wearing apparel, leather and related products
D16	Wood and products of wood and cork
D17T18	Paper products and printing
D19	Coke and refined petroleum products
D20T21	Chemicals and pharmaceutical products
D22	Rubber and plastic products
D23	Other non-metallic mineral products
D24	Basic metals
D25	Fabricated metal products
D26	Computer, electronic and optical products
D27	Electrical equipment
D28	Machinery and equipment, nec
D29	Moto vehicles, trailers and semi-trailers
D30	Other transport equipment
D31T33	Other manufacturing; repair and installation of machinery and equipment
D35T39	Electricity, gas, water supply, sewerage, waste and remediation services
D41T43	Construction
D45T47	Wholesale and retail trade; repair of motor vehicles
D49T53	Transportation and storage
D55T56	Accommodation and food services
D58T60	Publishing, audiovisual and broadcasting activities
D61	Telecommunications
D62T63	IT and other information services
D64T66	Financial and insurance activities
D68	Real estate activities
D69T82	Other business sector services
D84	Public administration and defence; compulsory social security
D85	Education
D86T88	Human health and social work
D90T96	Arts, entertainment, recreation and other service activities
D97T98	Private households with employed persons

Appendix C: Cyber Risk Taxonomy

The aim of a classification or taxonomy is to provide a practical and consistent framework for categorizing, understanding, and comparing cyber risk scenarios (Hansman and Hunt, 2005).[10] Early taxonomies such as Bishop's (1995) concentrated on categorizing security vulnerabilities in software to assist security practitioners in maintaining secure systems. Howard (1997) analyzed 4,299 cyber incidents and not only classified them according to the categories attacker, target, and result, but also included intangible factors such as the attacker's motivation. The cyber-attack taxonomy proposed by Hansman and Hunt (2005) is based on four dimensions (i.e., attack vector, attack targets, vulnerabilities, and payloads[11]), whereby additional dimensions can be added as needed. While almost any cyber-attack can be categorized by these taxonomies, only the one developed by Applegate and Stavrou (2013) is capable of illustrating the complex interactions between attackers, actors and other potentially related events. Even though a wide array of taxonomies exists, none is able to capture all aspects of every conceivable cyber risk perfectly.

In this paper, Howard's (1997, 2015) taxonomy is applied to classify different cyber risk scenarios. This common language is widely accepted because it is simple and is used by incident response teams as well as by the US Department of Defense. In comparison to the taxonomies discussed above, it also includes more intangible factors such as an attacker's motivation. Additionally, the broad taxonomy considers the whole attack process. This is especially useful

---

[10] Satisfactory taxonomies should have classification categories with the following six characteristics: mutually exclusive, exhaustive, unambiguous, repeatable, accepted (i.e., logical and intuitive), and useful (i.e., provides an insight into the field of inquiry) (Amoroso, 1994). A taxonomy is, however, only an approximation of reality and might be inadequate in some respects.

[11] Payloads are the malicious mechanisms that exploit the vulnerability of a system (Yadav and Rao, 2015).

when classifying cyber risk scenarios as they usually describe the entire attack process. Furthermore, while the categories of the taxonomy are given, the characteristics are diverse and may be extended if technical developments should make it necessary.

Howard's (1997, 2015) taxonomy classifies cyber risk scenarios by seven categories: attacker(s), tool, vulnerability, action, target, unauthorized result, and objectives (see Figure 4). While cyber incidents are characterized by all categories, the actual cyber-attacks are only described by the categories 2–5 and the cyber events by the categories 4–5. The dotted arrow indicates that an incident may be comprised of a single or multiple attacks. The definitions of the different characteristics of the taxonomy are given in Table 7.

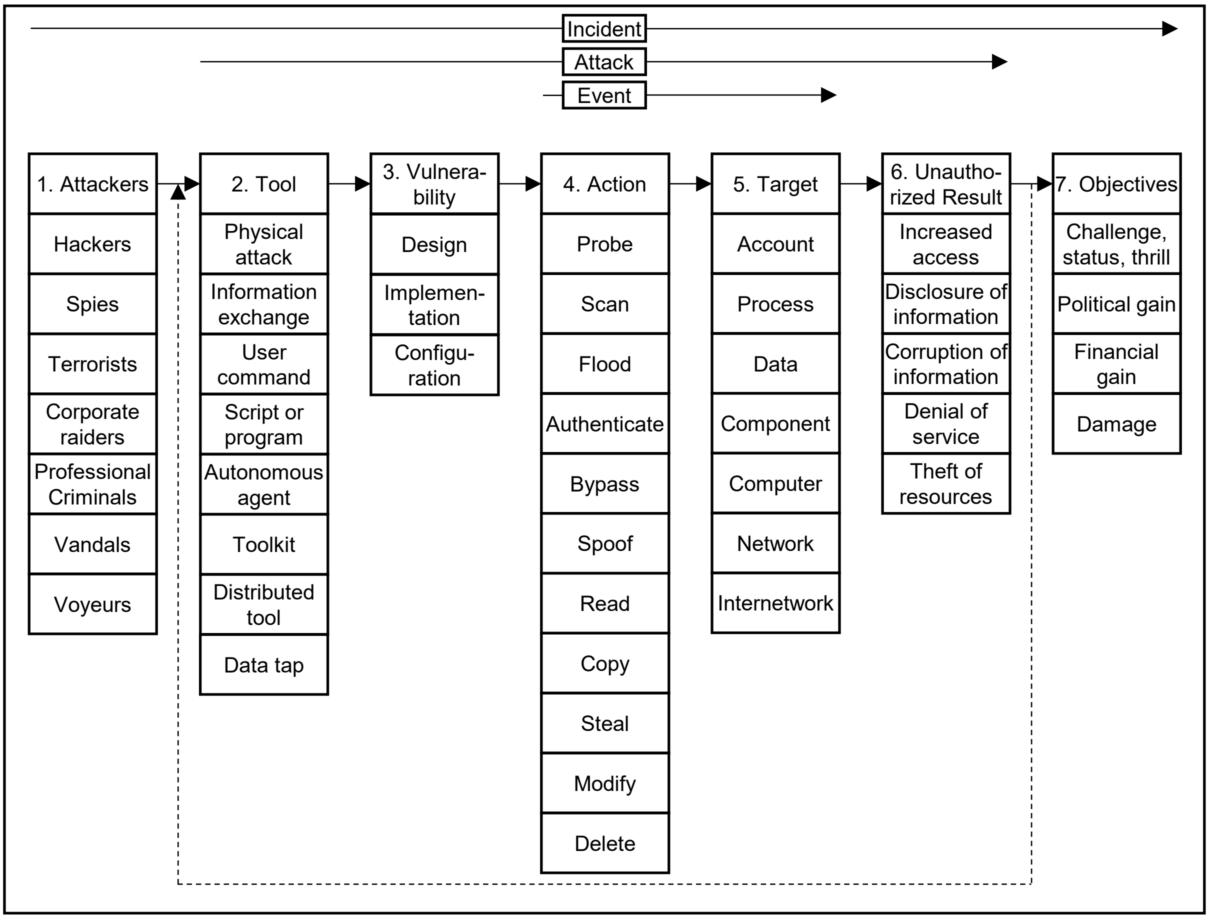

Figure 4. Computer and Network Incident Information Taxonomy (Howard, 2015)

Table 8. Definitions of the Characteristics of the Computer and Network Incident Information Taxonomy (Howard, 2015)

Characteristic	Definition
Incident	Group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.
Attack	A series of steps taken by an attacker to achieve an unauthorized result.
Event	Action directed at a target that is intended to result in a change of state, or status, of the target.
Attackers	Individual who attempts one or more attacks in order to achieve an objective.
Hackers	Attackers who attack computers for challenge, status, or the thrill of obtaining access.
Spies	Attackers who attack computers for information to be used for political gain.
Terrorists	Attackers who attack computers to cause fear, for political gain.
Corporate raiders	Employees (attackers) who attack competitors' computers for financial gain.
Professional criminals	Attackers who attack computers for personal financial gain.
Vandals	Attackers who attack computers to cause damage.
Voyeurs	Attackers who attack computers for the thrill of obtaining sensitive information.
Tool	Means of exploiting a computer or network vulnerability.
Physical attack	Means of physically stealing or damaging a computer, network, its components, or its supporting systems (e.g., air conditioning, electric power, etc.).
Information exchange	Means of obtaining information either from other attackers (e.g., through an electronic bulletin board) or from the people being attacked (commonly called social engineering).
User command	Means of exploiting a vulnerability by entering commands to a process through direct user input at the process interface. An example is entering UNIX commands through a telnet connection or commands at a protocol's port.
Script or command	Means of exploiting a vulnerability by entering commands to a process through the execution of a file of commands (script) or a program at the process interface. Examples are a shell script to exploit a software bug, a Trojan horse log-in program, or a password-cracking program.
Autonomous agent	Means of exploiting a vulnerability by using a program or program fragment that operates independently from the user. Examples are computer viruses or worms.
Toolkit	Software package that contains scripts, programs, or autonomous agents that exploit vulnerabilities. An example is the widely available toolkit called rootkit.
Distributed tool	Tool that can be distributed to multiple hosts, which then can be coordinated to anonymously perform an attack on the target host simultaneously after some time delay.
Data tap	Means of monitoring the electromagnetic radiation emanating from a computer or network using an external device.
Vulnerability	Weakness in a system allowing unauthorized action.
Design	Vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability.
Implementation	Vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design.
Configuration	Vulnerability resulting from an error in the configuration of a system, such as having system accounts with default passwords, having "world write" permission for new files, or having vulnerable services enabled.
Action	Step taken by a user or process in order to achieve a result,11 such as to probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify, or delete.
Probe	Access a target in order to determine one or more of its characteristics.
Scan	Access a set of targets systematically in order to identify which targets have one or more specific characteristics.
Flood	Access a target repeatedly in order to overload the target's capacity.
Authenticate	Present an identity to a process and, if required, verify that identity, in order to access a target.
Bypass	Avoid a process by using an alternative method to access a target.
Spoof	Masquerade by assuming the appearance of a different entity in network communications.

Read	Obtain the content of data in a storage device or other data medium.
Copy	Reproduce a target leaving the original target unchanged.
Steal	Take possession of a target without leaving a copy in the original location.
Modify	Change the content or characteristics of a target.
Delete	Remove a target or render it irretrievable.
Target	Computer or network logical entity (account, process, or data) or a physical entity (component, computer, network or internetwork).
Account	Domain of user access on a computer or network that is controlled according to a record of information, which contains the user's account name, password, and use restrictions.
Process	Program in execution, consisting of the executable program, the program's data and stack, its program counter, stack pointer and other registers, and all other information needed to execute the program.
Data	Representations of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. Data can be in the form of files in a computer's volatile memory or nonvolatile memory, or in a data storage device, or in the form of data in transit across a transmission medium.
Component	One of the parts that make up a computer or network.
Computer	Device that consists of one or more associated components, including processing units and peripheral units, that is controlled by internally stored programs and that can perform substantial computations, including numerous arithmetic operations or logic operations, without human intervention during execution. Note: may be stand-alone or may consist of several interconnected units
Network	Interconnected or interrelated group of host computers, switching elements, and interconnecting branches.
Internetwork	Network of networks.
Unauthorized result	Unauthorized consequence of an event.
Increased access	Unauthorized increase in the domain of access on a computer or network.
Disclosure of information	Dissemination of information to anyone who is not authorized to access that information.
Corruption of information	Unauthorized alteration of data on a computer or network.
Denial of service	Intentional degradation or blocking of computer or network resources.
Theft of resources	Unauthorized use of computer or network resources.
Objectives	Purpose or end goal of an incident.

Appendix D: Cyber risk scenarios

Table 1. Summary of Scenarios

No	Scenario	Authors	Description/Attack goal	When*	Where*	What*	How*	Threat actor	Estimated frequency	Estimated severity / economic impact	Required know-how and resources of attackers	Persistence of the attack	Example
1	Supervisory control and data acquisition network/ industrial control system extortion	Dejung (2017)	In a supervisory control and data acquisition network/industrial control system extortion scenario, simple process variables are maliciously modified to change the product properties. Victims are e.g. critical infrastructure providers (i.e., electric grid, oil/gas/water networks).	Exploit	Administrative Interface	Manipulate Timing and State	e.g. Stuxnet	Politically, economically or religiously motivated state sponsored attackers (potentially supported by insiders).	n.a.	Economic impact is estimated at 0.05% to 0.3% of GDP, caused mainly by business interruption, loss of profit, and physical damages including accidents and fatalities.	Process know-how and remote access to the industrial control system are necessary.	Potential to persist for three weeks.	The first supervisory control and data acquisition network/industrial control system attack was on Maroochy Shire Wastewater Treatment Plant in Australia (Abrams and Weiss, 2008).
2	Cloud Service Provider Failure	Risk Management Solutions Inc. (2016); Dejung (2017); World Economic Forum (2014)	Business operations of many companies are disrupted due to unavailability of major cloud service provider (CSP) company. The outage is on a scale never experienced by a commercial CSP.	Control	Cloud Web Interface	Credential Access	e.g. John the Ripper	Criminals with the goal of earning money through extortion.	Very low as the big four CSP typically achieve over 99.9% reliability of service. However, due to insufficient observational data, an assessment of the likelihood of a catastrophic failure of these systems is not possible through statistical means.	n.a. (It is expected that 17,500 companies are unable to access cloud services.)	Relatively little know-how and resources needed if the attack is executed via a Distributed-Denial-of-Service attack.	A few hours up to one month of persistence are conceivable.	In 2016, the world's largest Software-as-a-Service (SaaS) customer relationship management provider, Salesforce, experienced a system outage that lasted more than two business days, resulting in customers losing four hours of CRM data (Nicastro, 2016).
3	Health sector and hospitals scenarios	Dejung (2017)	A sophisticated cyber-attack that infiltrates several hospitals and becomes active at the same time, resulting in non-availability of hospitals for two to three weeks.	Control	Device Network Services/Device Web Interface	Command and Control	e.g. WannaCry	Politically or economically state sponsored attackers or highly sophisticated terrorists or criminals.	Likelihood of successful attacks that affect more than 10% of a country's hospitals is assumed to be low to medium as architecture, implementation, and configuration of	Max. economic impact is assumed to be 0.2% of GDP.	Complex design and execution require a lot of know-how, infrastructure, and personnel.	Potential to persist for two to three weeks.	In 2017, a massive ransomware, known as WannaCry, attack has shut down work at 16 hospitals across the UK (Brandom, 2017).

									the malware are individual.				
4	Municipal services compromised	Trautman and Ormerod (2018)	Malware is deployed on city administrative service systems, disabling civil services functions for an entire city.	Exploit	Device Network Services	Subvert Access Control	e.g. SamSam	Politically motivated state sponsored attackers. Also, criminals pursuing extortion.	n.a.	Estimates from the SamSam ransomware attack on the city of Atlanta indicate that the total cost of disturbance was around $20m.	Attackers only need to design a phishing email relevant to city employees that will prompt civil servants to download or open an infected file with the ransomware.	Persistence can be indefinite if the attack is not entirely remediated as ransomware can lay dormant in systems.	In 2018, the city of Atlanta was infected with the SamSam ransomware. The city decided not to pay the $51,000 payment and instead took city services offline for over a week, incurring costs of around $17m for restoring the IT infrastructure (Armerding, 2018).
5	Telecommunication scenarios	Dejung (2017)	Malware targets e.g. a router or modem with 50% market share and results in the deletion of the firmware whereby the devices must be replaced.	Exploit	Device Firmware/ Device Web Interface	Manipulate System Resources	e.g. BCMUPnP_Hunter	Criminals (with the aim of earning money through extortion) or politically, economically or religiously motivated state sponsored attackers.	n.a.	0.35% of GDP in the first scenario and 0.03% in the second scenario.	The second scenario requires less time and resources than the first on. However, a Border Gateway Protocol (BGP) attack might require less know-how and is therefore to be expected more frequently.	Attack persistence of seven days is assumed in the first scenario, while the persistence in the second scenario is expected to be shorter.	In 2017, the Spanish telecommunication company Telefónica was affected by the ransomware WannaCry (Teoh et al., 2018).
6	Strategic cross-sector attack scenario	Risk Management Solutions Inc. (2016); Ruffle et al. (2014)	The aim of this scenario is to take hostage of many companies by disabling IT functionality to obtain payoffs. Many enterprises are attacked, and high ransom payments are demanded.	Control	Device Network Services	Command and Control	e.g. NotPetya	Criminals with the goal of earning money through extortion.	Ruffle et al. (2014) estimate the frequency of such an event at one percent.	According to Ruffle et al. (2014) the overall global loss is estimated between $4.5 trillion to $15 trillion. Additionally, they predict a plunge of the financial markets similarly to the financial crisis in 2008.	Design and implementation of ransomware targeted at companies takes time and requires sophisticated programmers.	Relatively short perception of a few days as the attack is expected to be carried out on a single day at numerous companies.	The three best-known ransomware versions currently in use are CryptoWall, CTB-Locker and TorrentLocker (Richardson and North, 2017).

Note: The criteria marked with * are adopted from the attack anatomy proposed by Falco et al. (2018).

Appendix E

Scenario 1: Supervisory Control and Data Acquisition Network/ICS Extortion

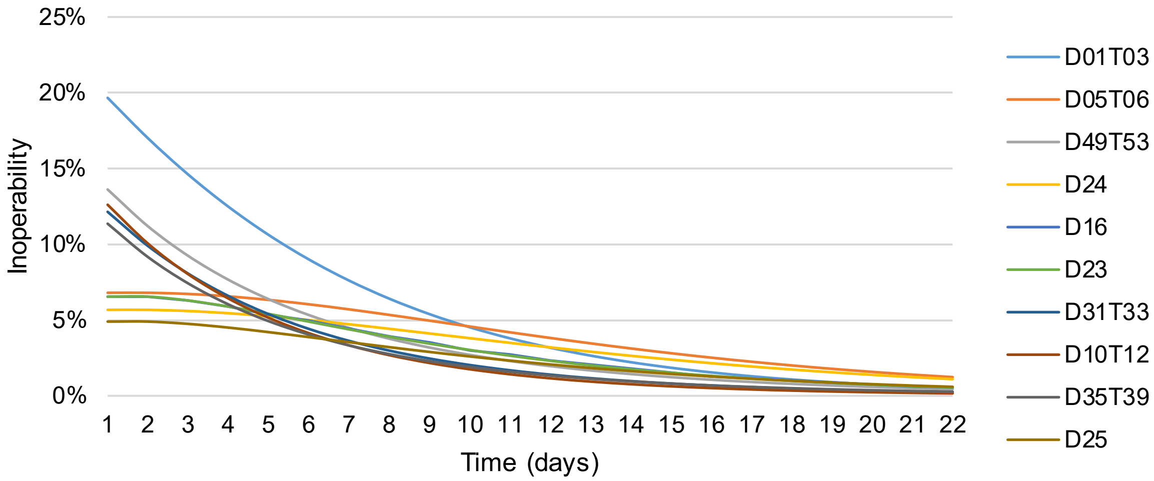

Figure 1. Inoperability Development of the Top 10 Inoperable Sectors

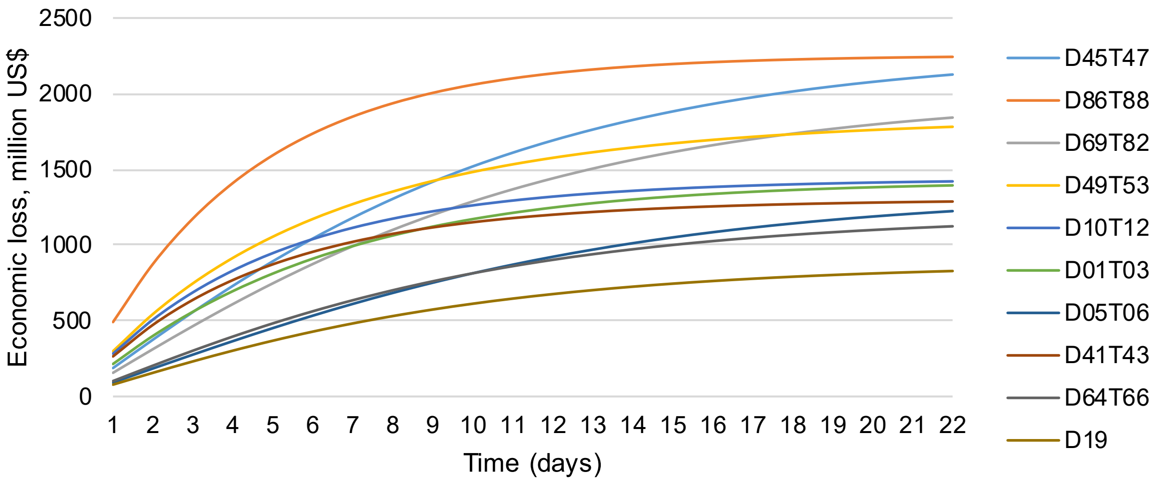

Figure 2. Cumulative Economic Losses for the Top 10 Affected Sectors

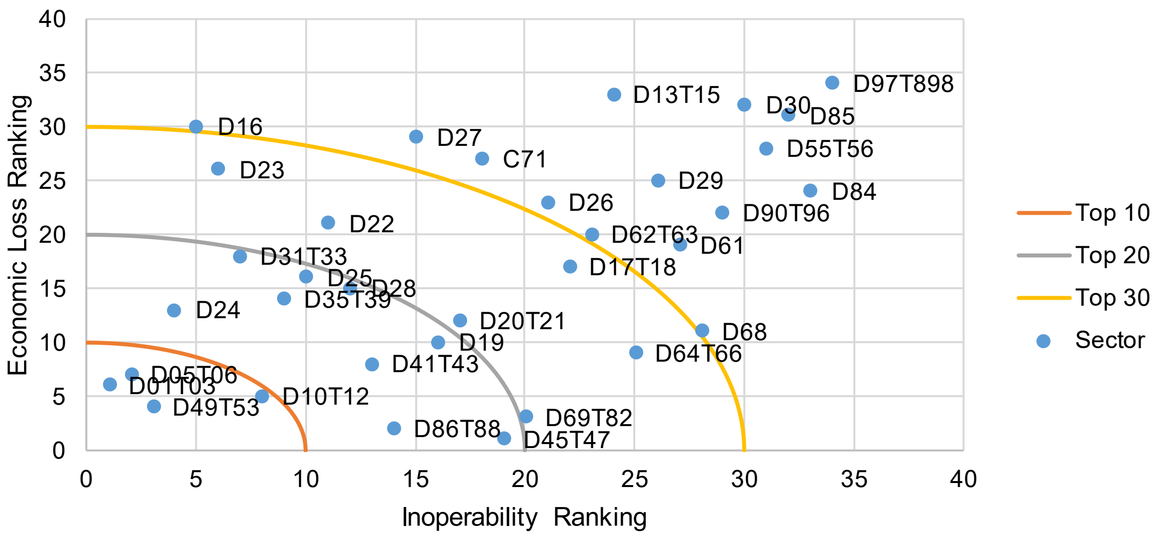

Figure 3. Dynamic Cross-Prioritization Plot

Scenario 2: Cloud Service Provider Failure

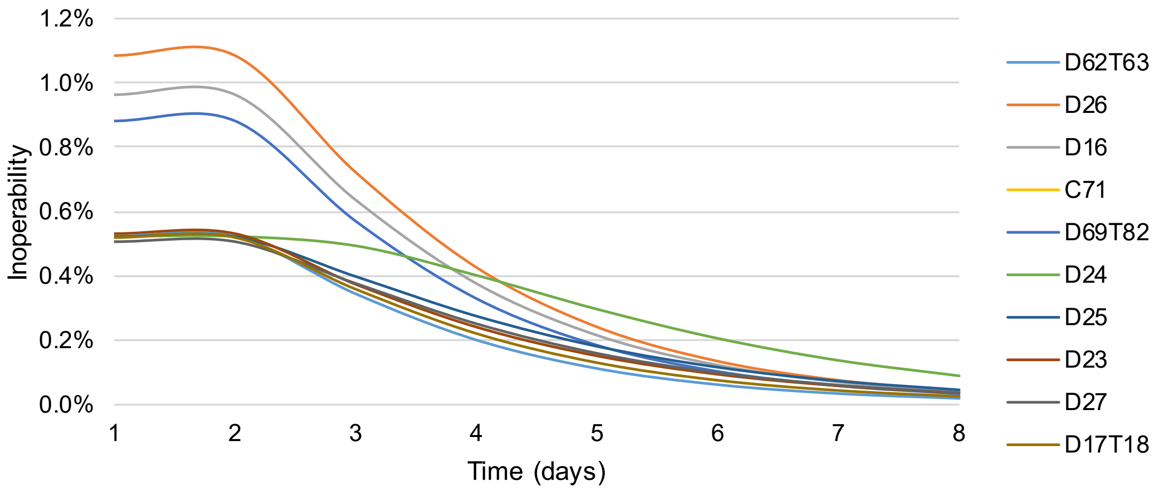

Figure 4. Inoperability Development of the Top 10 Inoperable Sectors

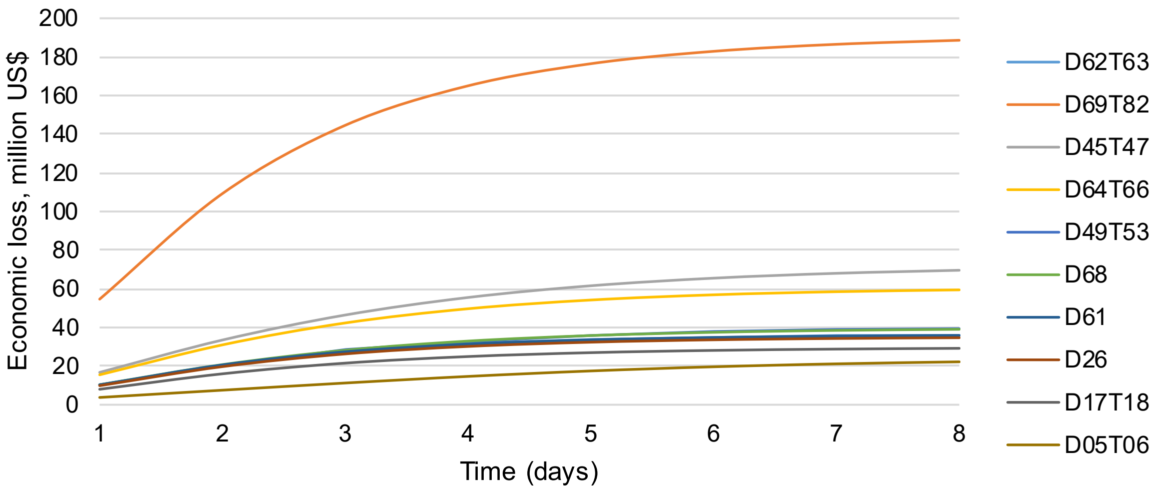

Figure 5. Cumulative Economic Losses for the Top 10 Affected Sectors

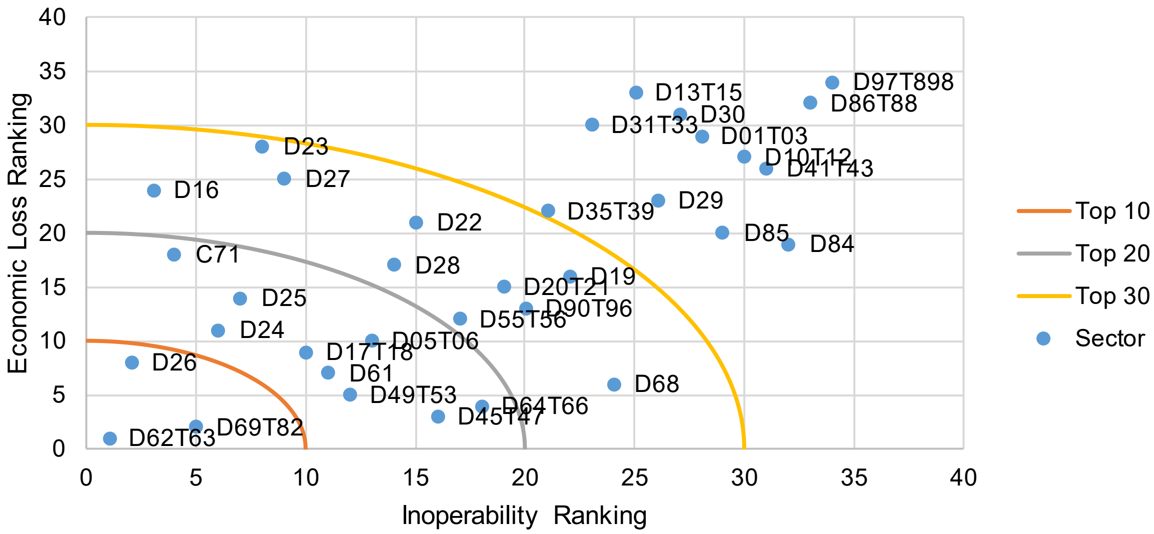

Figure 6. Dynamic Cross-Prioritization Plot

Scenario 3: Health Sector and Hospitals

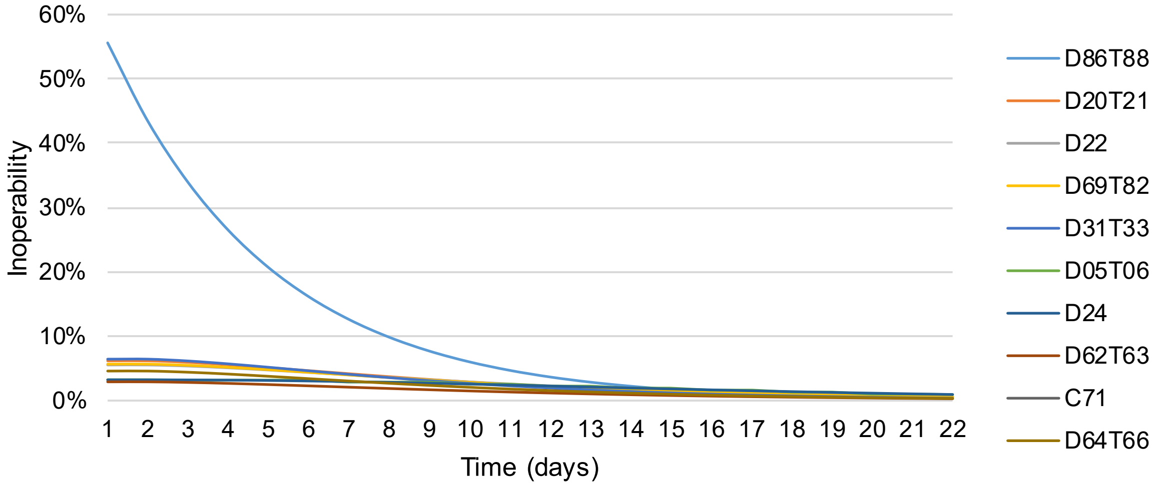

Figure 11. Inoperability Development of the Top 10 Inoperable Sectors

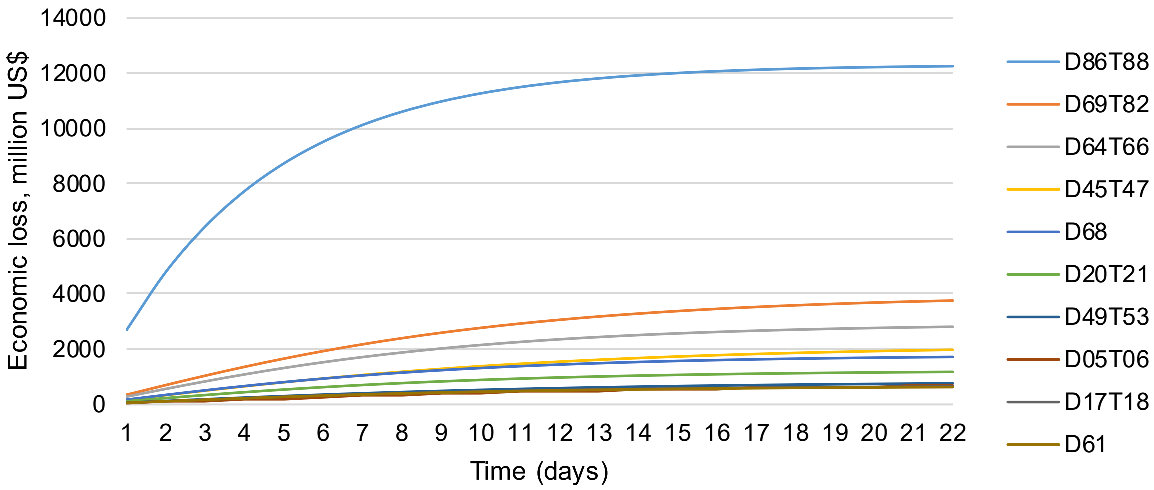

Figure 7. Cumulative Economic Losses for the Top 10 Affected Sectors

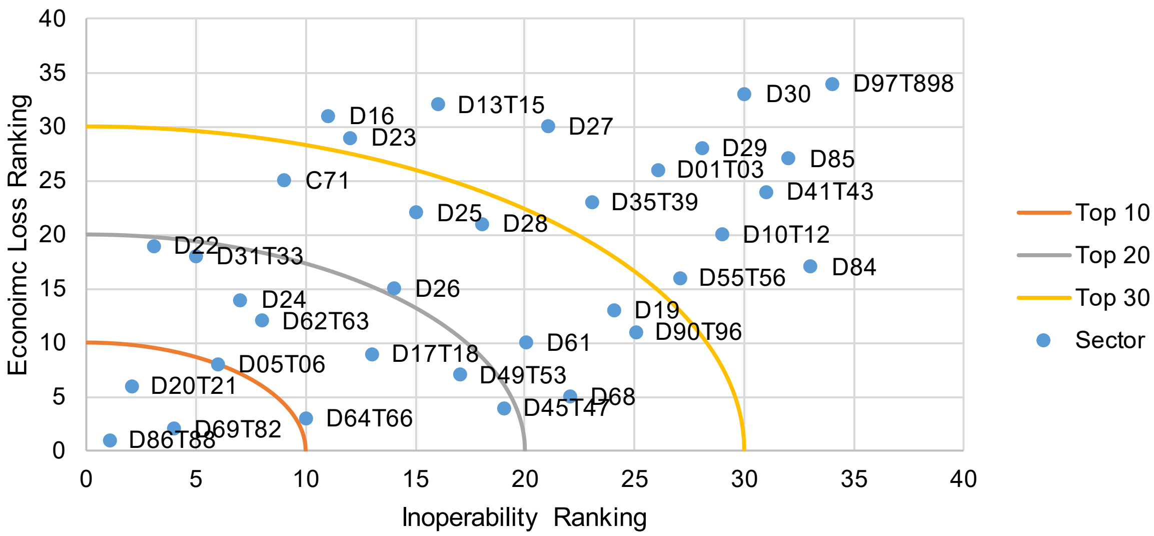

Figure 8. Dynamic Cross-Prioritization Plot

Scenario 4: Municipal Services

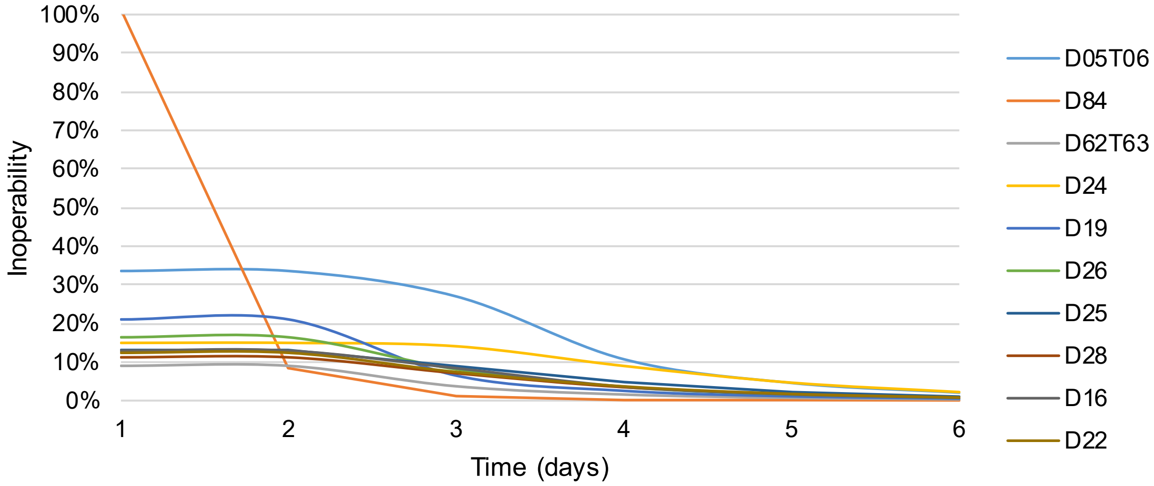

Figure 9. Inoperability Development of the Top 10 Inoperable Sectors

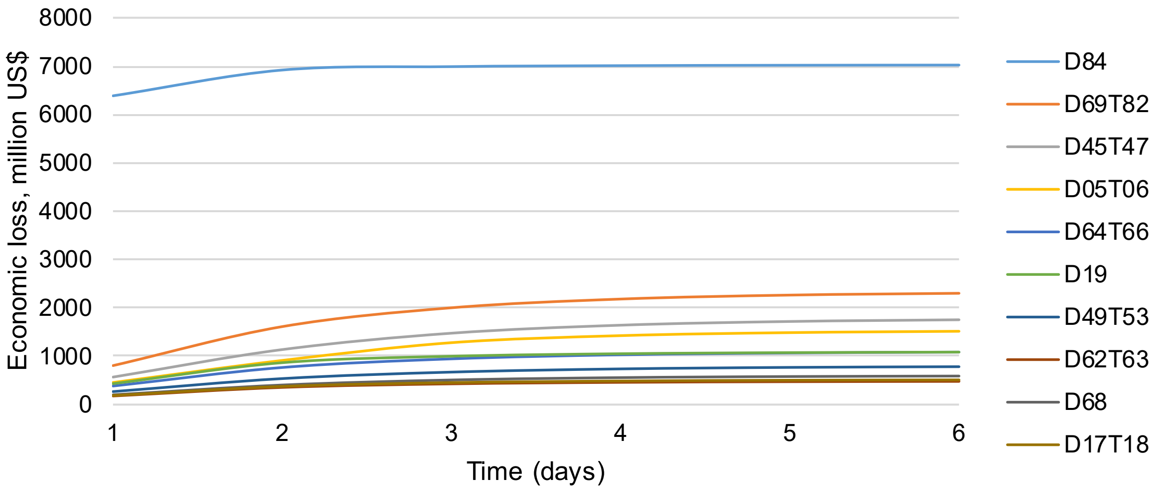

Figure 10. Cumulative Economic Losses for the Top 10 Affected Sectors

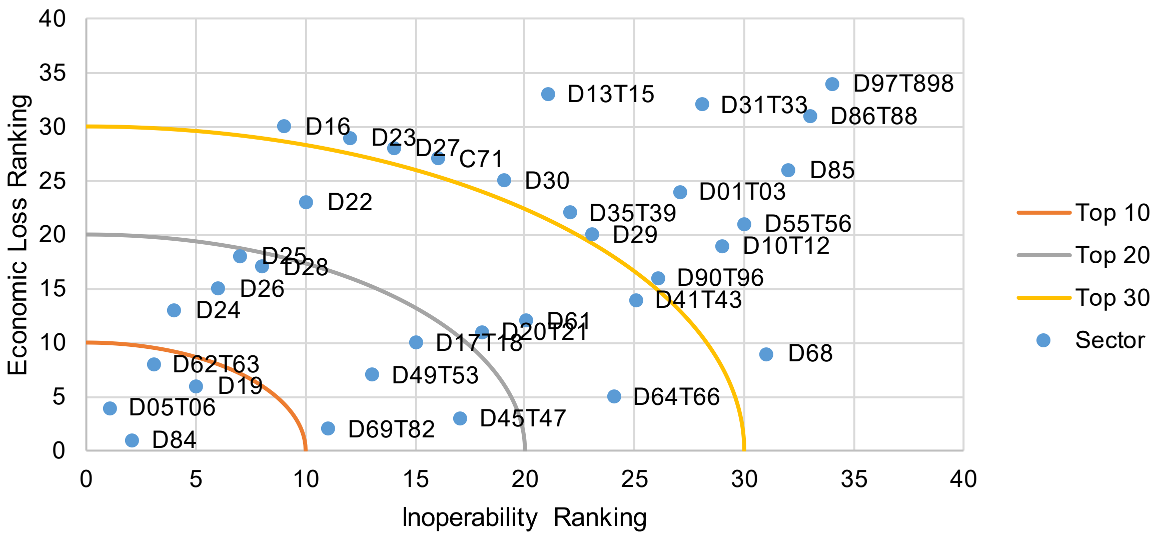

Figure 11. Dynamic Cross-Prioritization Plot

Scenario 5: Telecommunication

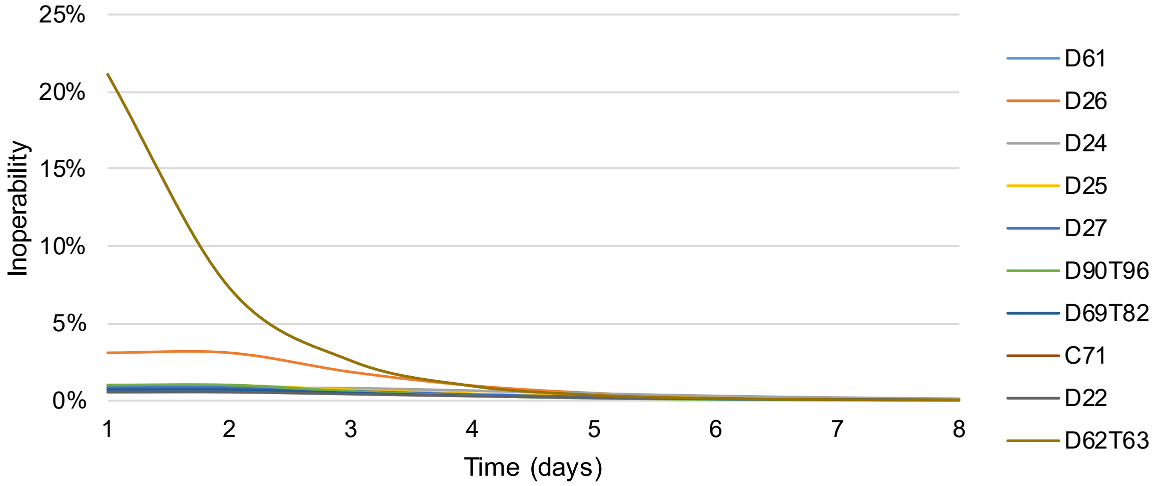

Figure 17. Inoperability Development of the Top 10 Inoperable Sectors

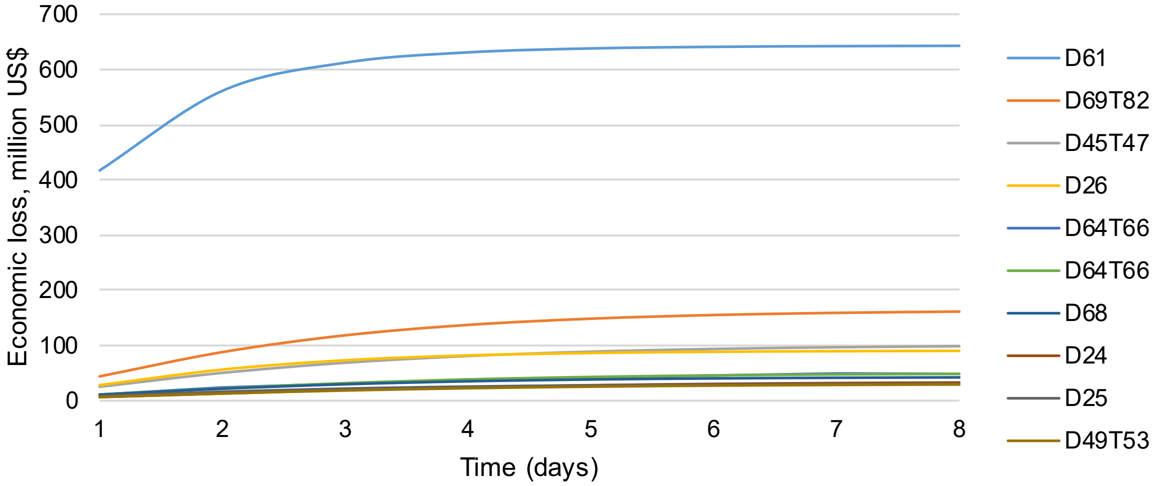

Figure 18. Cumulative Economic Losses for the Top 10 Affected Sectors

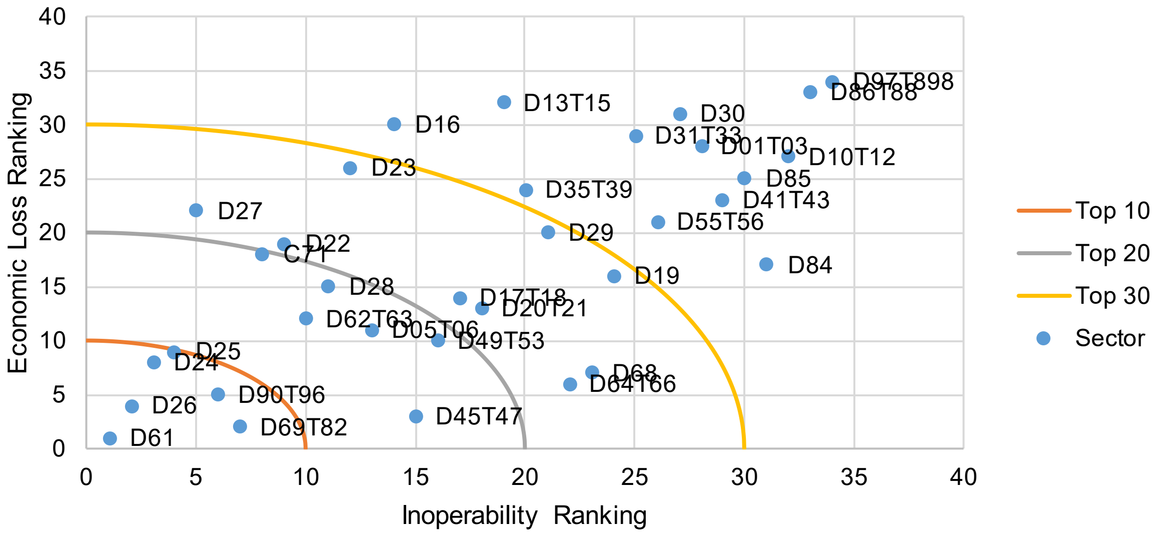

Figure 19. Dynamic Cross-Prioritization Plot

Scenario 6: Cross-Sector Attack

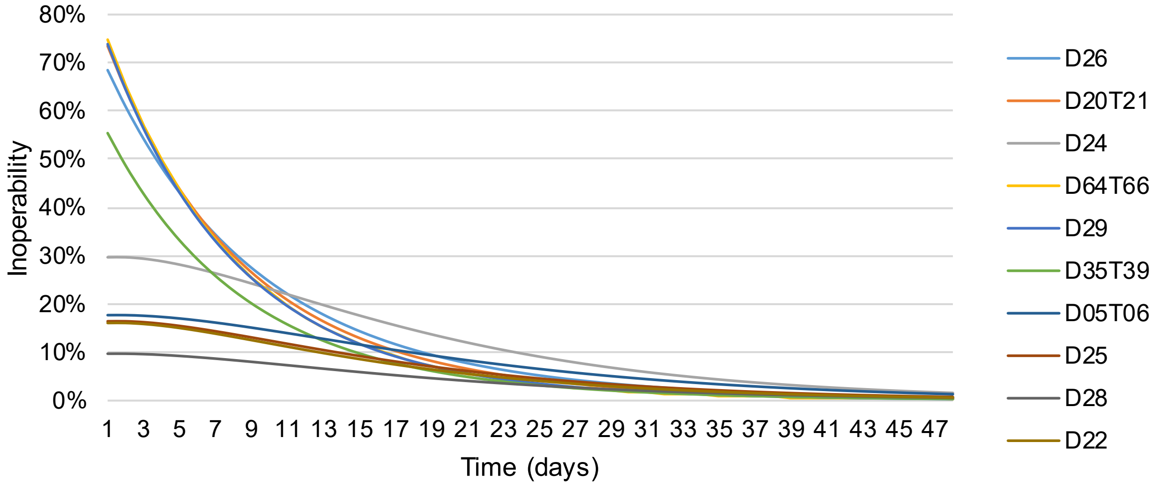

Figure 12. Inoperability Development of the Top 10 Inoperable Sectors

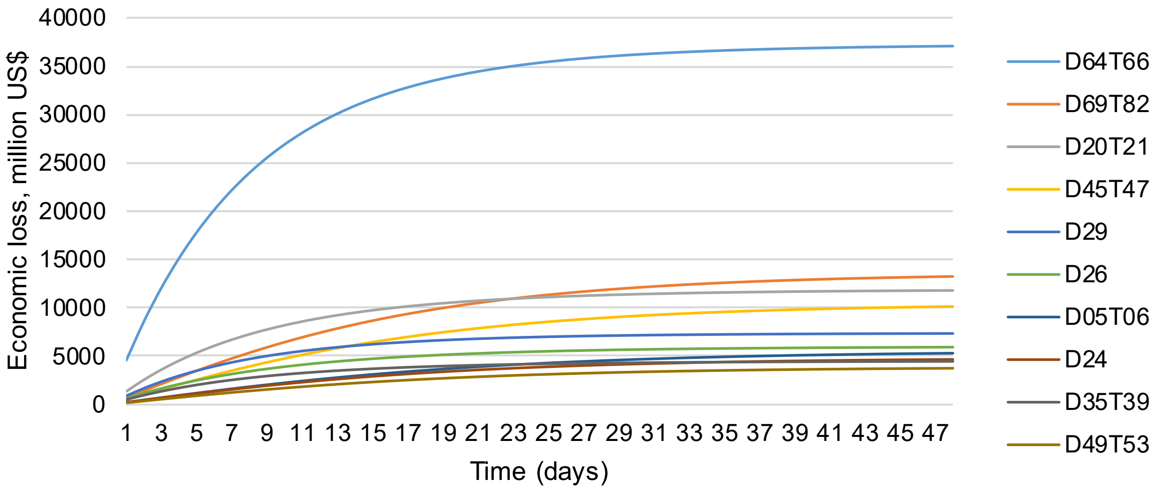

Figure 13. Cumulative Economic Losses for the Top 10 Affected Sectors

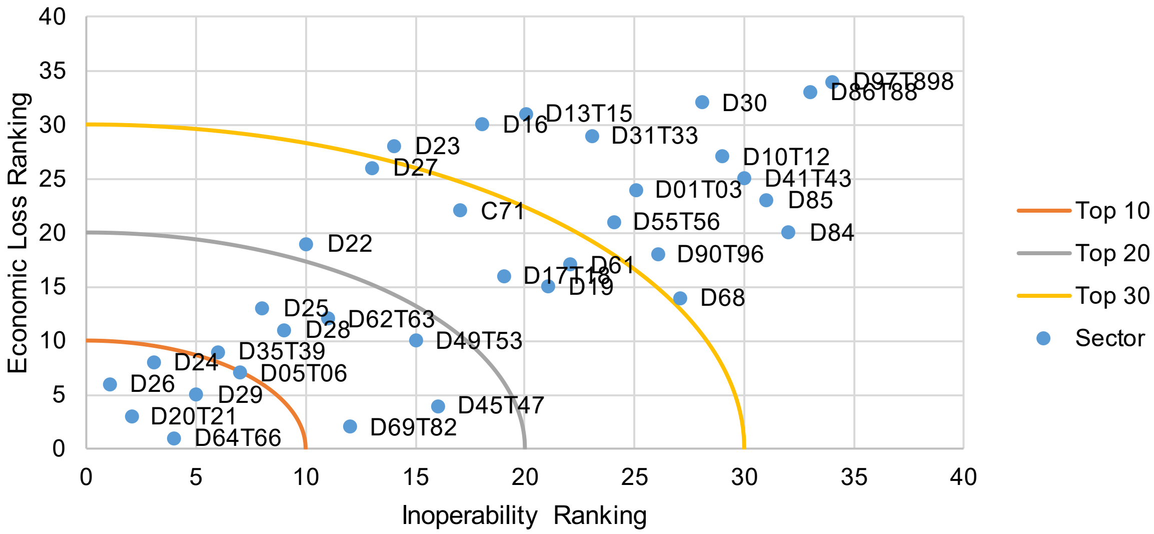

Figure 14. Dynamic Cross-Prioritization Plot

Appendix F: Calculation of Loss Estimators

In this Appendix we show the calculation of the economic loss considering scenario 1 as example. The first step is the definition of three input parameters (see Table 3 in the main body of the paper and Table 11 below), i.e. information on which sectors are affected, their initial inoperability and their recovery time. These input parameters together with the Input-Output Table for the United States (Table 12 below) are all parameters necessary to derive the economic loss for the respective scenario, which is the second step of the analysis. One key aspect in the calculations in the second step are the ripple effects from one sector to another. Considering scenario 1 as an example, although only seven sectors are directly affected, we see that also numerous other sectors are affected, because they are linked with each other in the input-output table. The inoperability of a sector then goes down over time and is driven by not only be the own recovery rate, but again also by the interdependence with the other sectors, leading to the development of inoperability over time presented in Figure 1. The economic loss of a particular sector on a certain day is then calculated as the inoperability on that day times the output of the respective sector on that day. Finally, all losses are cumulated across sectors and across time. Table 10 illustrates the two steps necessary to derive the loss estimates.

Table 10. Steps to obtain Loss Estimates

Step	Sub-steps
Step 1: Estimate input parameters	a) Sectors which are affected b) their initial level of inoperability c) their recovery time
Step 2: Calculate economic loss	a) Determine daily Input-Output Table with elements x_{ij} (yearly numbers (Table 12) divided by 365) b) Calculate technical coefficient matrix $\boldsymbol{A}$ with elements $a_{ij} = x_{ij}/x_j$ and x_j= total production output of sector j c) Calculate interdependency matrix $\boldsymbol{A}^* = \hat{\boldsymbol{x}}^{-1}\boldsymbol{A}\hat{\boldsymbol{x}}$ with $\hat{\boldsymbol{x}}$ = diagonal matrix generated by the vector $\bar{\boldsymbol{x}}$ (industry total output) and elements $a^*_{ij} = a_{ij}\, x_j/x_i$ d) Calculate $(\boldsymbol{I} - \boldsymbol{A}^*)^{-1}$ with $\boldsymbol{I}$ = identity matrix e) Calculate inoperability vector $\boldsymbol{q}(0)$ (ratio of unrealized production with respect to "business-as-usual" production on day 0, i.e. the day of pertubation) = $[\boldsymbol{I} - \boldsymbol{A}^*]^{-1}\boldsymbol{c}^*$ and development in the following days $\boldsymbol{q}(t+1) = \boldsymbol{K}\boldsymbol{A}^*\boldsymbol{q}(t) + \boldsymbol{K}\boldsymbol{c}^*(t) + (\boldsymbol{I}-\boldsymbol{K})\boldsymbol{q}(t)$ with $\boldsymbol{q}(t)$ = inoperability vector at time t, $\boldsymbol{K}$ = sectoral resilience matrix, and $\boldsymbol{c}^*(t)$ = perturbation vector at time t f) Calculate economic loss per day and per sector $\boldsymbol{q}(t)\ x_i$ g) Aggregate economic losses across sectors and days

All data and details of the calculation are presented in an excel spreadsheet which is available in the supplemental material; the spreadsheet also contains a simple example with only three sectors to help clarifying all calculations. For more technical details, we also refer to the references we cite in the main body of the text (Miller and Blair, 2009; Lian et al., 2007; Santos, 2006; Lian and Haimes, 2006). It is obvious that the calculations rely on manifold simplifying assumptions, but still we believe that the input-output model provides a simple, understandable, transparent and replicable way to assess potential losses from the scenarios at hand.

Table 11. Input Parameters for Scenario 1

Sector	Triangular distribution of inoperability c			Recovery period (days)
	min	Mode	max	
D01T03	0.05	0.10	0.15	21
D05T06	0.00	0.00	0.00	21
D10T12	0.05	0.10	0.15	21
D13T15	0.00	0.00	0.00	21
D16	0.00	0.00	0.00	21
D17T18	0.00	0.00	0.00	21
D19	0.00	0.00	0.00	21
D20T21	0.00	0.00	0.00	21
D22	0.00	0.00	0.00	21
D23	0.00	0.00	0.00	21
D24	0.00	0.00	0.00	21
D25	0.00	0.00	0.00	21
D28	0.00	0.00	0.00	21
D26	0.00	0.00	0.00	21
D27	0.00	0.00	0.00	21
D29	0.00	0.00	0.00	21
D30	0.00	0.00	0.00	21
D31T33	0.05	0.10	0.15	21
D35T39	0.05	0.10	0.15	21
D41T43	0.05	0.10	0.15	21
D45T47	0.00	0.00	0.00	21
D55T56	0.00	0.00	0.00	21
D49T53	0.05	0.10	0.15	21
D61	0.00	0.00	0.00	21
D64T66	0.00	0.00	0.00	21
D68	0.00	0.00	0.00	21
C71	0.00	0.00	0.00	21
D62T63	0.00	0.00	0.00	21
D69T82	0.00	0.00	0.00	21
D84	0.00	0.00	0.00	21
D85	0.00	0.00	0.00	21
D86T88	0.05	0.10	0.15	21
D90T96	0.00	0.00	0.00	21
D97T898	0.00	0.00	0.00	21

Table 12. Input-Output Table for all Scenarios (per annum, in USD million, taken from https://stats.oecd.org/Index.aspx?DataSetCode=IOTS)

	D01T03	D05T06	D10T12	D13T15	D16	D17T18	D19	D20T21	D22	D23	D24	D25	D28	D26	D27	D29
D01T03	69955	135	184482	470	8036	4853	24	6718	3031	8	3	9	3	7	16	23
D05T06	3410	30092	2026	102	56	3399	438256	19245	349	11060	37670	644	404	33	220	326
D10T12	21508	145	116549	522	66	1909	426	4571	343	77	113	105	111	32	39	202
D13T15	258	55	235	6059	337	3649	108	751	1552	229	46	44	584	37	21	3797
D16	554	112	368	47	11530	5803	21	320	812	229	337	178	560	209	171	1738
D17T18	546	1276	21397	727	552	110508	481	7023	4250	1396	2178	2603	2290	1638	1024	3198
D19	19975	9038	3655	502	603	5630	13308	26446	2761	1029	2726	1408	1558	494	1093	382
D20T21	14374	5416	6605	8511	1436	18315	5959	172304	39601	3128	2054	5449	3275	3528	2017	5470
D22	1515	1904	16078	405	442	4188	227	3162	12662	868	973	1863	6065	1916	1169	18010
D23	70	1065	3795	137	555	394	383	1271	1028	8119	2780	909	1335	427	1112	4399
D24	196	5127	5485	288	401	764	1224	944	2001	1036	101668	59878	31566	5602	19278	37326
D25	1983	4157	13545	522	1722	7953	345	7244	4899	2013	7056	28882	21791	7040	6448	27293
D28	5293	26275	5858	96	658	5218	406	7220	3011	569	3675	5907	48667	1368	3154	35267
D26	169	763	3385	522	511	9075	401	4904	1846	998	2593	3776	6801	37581	3454	14287
D27	415	237	1014	52	373	569	94	364	640	136	2190	1684	3030	3290	5795	3428
D29	584	1378	2347	93	344	1688	126	1115	422	397	337	1163	3854	744	339	126525
D30	92	370	396	47	54	446	91	438	115	55	147	294	760	257	102	330
D31T33	212	258	542	175	406	1539	254	932	346	221	7173	275	1515	350	255	1263
D35T39	2176	2678	4093	300	411	4561	2220	7832	1124	1613	4128	1731	329	436	342	1078
D41T43	2062	4829	1090	144	115	918	3487	973	284	233	571	455	332	501	134	326
D45T47	43811	29445	129805	10392	7901	48503	98314	76072	22043	8789	30138	19855	26282	17706	7921	52188
D55T56	298	712	2094	229	289	3359	231	913	729	410	544	1058	346	364	124	466
D49T53	3933	9269	28368	1543	2509	16817	12807	13685	4384	4763	12571	4929	4703	2531	1604	3008
D61	428	1706	2664	442	306	4864	567	2675	766	459	551	1390	1305	1987	351	1042
D64T66	10889	6812	5908	1523	491	3471	203	3424	1761	1258	2674	3556	3456	1687	946	1860
D68	16053	490	655	147	107	3396	57	1611	241	104	146	582	439	1266	126	346
C71	1414	4577	2082	201	126	3369	297	2590	454	314	469	1115	1083	1182	291	750
D62T63	518	2635	3505	562	524	9880	344	2547	1067	722	1010	2543	3342	2457	373	1174
D69T82	2332	22628	34489	5169	3170	43311	5718	43762	7778	4969	3592	14457	12455	16653	3834	17425
D84	1597	1661	4554	364	364	4129	1372	4168	767	704	1730	1131	1002	766	359	1056
D85	238	980	1581	227	158	2114	354	1774	384	239	411	594	529	711	164	729
D86T88	245	310	717	59	48	445	409	502	132	60	156	159	179	143	49	260
D90T96	531	1402	3656	492	347	3527	1079	3768	880	614	1289	1363	957	1016	324	914
D97T898	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TXS_INT_FNL: Taxes less subsidies on intermediate and final products	-406	919	-4170	358	140	704	2756	1822	421	261	585	430	577	160	178	390
TTL_INT_FNL: Total intermediate and final expenditure at purchasers' prices	233427	230856	608856	41425	45086	345368	594150	438588	122884	57077	239986	180516	202587	115215	62826	372774
VALU: Value added at basic prices	165139	265664	209376	28506	21698	217123	158291	240295	64682	31050	46832	116347	125207	216745	44445	72384
OUTPUT: Output	398566	496520	818233	69932	66785	562491	752441	678883	187566	88127	286818	296863	327793	331960	107271	445158

	D30	D31T33	D35T39	D41T43	D45T47	D55T56	D49T53	D61	D64T66	D68	C71	D62T63	D69T82	D84	D85
D01T03	4	336	6	1326	4317	6048	71	118	42	175	8	15	1120	2878	674
D05T06	283	344	34095	17628	874	1212	7371	345	224	7596	378	151	2286	32124	725
D10T12	68	117	43	255	5331	61564	547	114	214	226	34	91	1359	26182	18355
D13T15	406	2909	13	862	4282	610	152	178	63	105	90	33	563	2639	140
D16	188	5533	4	19252	2812	3361	1208	487	110	3280	591	1499	918	2946	229
D17T18	1481	3456	477	3883	30136	10179	4104	3139	20482	5881	1377	6015	30009	37762	7329
D19	579	1171	5224	48299	9065	5302	100138	527	2228	1944	747	530	7470	125832	3021
D20T21	1675	5417	1335	6858	6026	2514	2004	2111	2116	6034	350	1050	17741	21611	2349
D22	2676	7134	36	15453	15294	7705	4571	2438	1431	925	724	698	5590	10176	3306
D23	339	758	108	33591	1182	4053	167	888	117	621	146	1044	3315	2903	379
D24	13154	12328	97	7220	2992	721	2069	487	72	1967	418	452	3226	1902	405
D25	11108	5504	243	49934	4306	8542	5688	8640	478	1920	731	2744	7181	13273	1520
D28	7858	2612	1171	38718	6543	3646	4028	2266	695	3417	773	1934	11383	10409	12584
D26	16856	3258	246	7421	14651	2172	1195	40287	7252	2232	599	8856	21021	28521	2858
D27	2650	951	40	21553	1313	2451	337	2657	286	565	222	1090	5508	4903	1973
D29	3604	761	32	6564	15371	1277	3257	850	1003	680	710	299	5876	13287	2900
D30	36539	167	76	753	1893	596	4075	518	1355	1180	148	493	2862	17934	400
D31T33	293	5348	37	4885	3004	1658	406	485	694	2466	160	713	2732	4104	352
D35T39	460	556	495	1512	9834	5536	2968	1473	1734	49545	259	706	4537	16438	19095
D41T43	205	206	2918	197	3170	1413	3273	2122	2408	117369	92	170	1353	54998	927
D45T47	15430	17998	9444	60956	100710	45421	40417	26276	18061	15953	6251	11032	40741	93844	21187
D55T56	374	343	559	1500	7496	4811	2358	2656	23327	6635	964	6413	20537	18128	5388
D49T53	3117	4426	5175	16384	92719	8393	76763	3724	19914	4094	1898	8277	28109	52016	3549
D61	1102	1379	485	4398	30369	6629	5412	103062	25766	15181	1834	9110	32984	38272	7658
D64T66	1670	2810	3959	7714	69324	15905	26585	5082	667377	72114	9528	8819	65785	61494	11440
D68	342	431	722	3561	100172	28824	13642	10408	20807	90006	2399	8523	49800	40198	56371
C71	740	337	322	5969	11527	3596	3457	3626	3726	1507	871	3974	14157	4467	3625
D62T63	2352	1727	1187	2931	22233	4779	3627	5509	42912	6450	4007	13421	45547	93469	9540
D69T82	15404	13642	7891	29597	223689	69782	33536	49009	151546	145425	14933	52328	234865	159410	33760
D84	710	353	567	1990	17971	6205	7732	3728	17143	18907	984	2813	13155	17786	7672
D85	561	620	408	1330	11244	3081	1584	2345	8685	6217	740	2852	11583	12707	4124
D86T88	121	134	73	498	1306	462	511	309	794	555	105	356	1484	9764	329
D90T96	707	365	735	4885	25208	10298	7305	39795	14279	14255	2272	3355	24843	35407	9803
D97T898	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TXS_INT_FNL: Taxes less subsidies on intermediate and final products	200	357	1434	6406	522	528	12211	-37	-781	2449	21	3	344	8267	2394
TTL_INT_FNL: Total intermediate and final expenditure at purchasers' prices	143352	108086	31984	434281	856884	339272	393268	325621	1056554	607876	55363	159859	719982	1076053	271857
VALU: Value added at basic prices	89005	100405	258952	493826	1447548	383627	408120	394740	1184488	1559669	112242	261682	1541701	1225316	772130
OUTPUT: Output	232357	208491	340937	928107	2304432	722899	301388	720361	2241042	2167544	167605	421542	2261683	2301369	1043987

	D86T88	D90T96	D97T898	HFCE: Households final consumption expenditure	NPISH: Non-profit institutions serving households	GGFC: General Government final consumption	GFCF: Gross Fixed Capital Formation	INVNT: Changes in inventories	CONS_ABR: Direct purchases abroad by residents (imports)	CONS_NONRES: Direct purchases by non-residents (exports)	EXPO: Exports (cross border)	IMPO: Imports (cross border)
D01T03	519	380	0	81330	192	0	597	-8323	132	32	61360	-32873
D05T06	1182	2540	0	11946	0	0	10366	-1909	74	149	32672	-263477
D10T12	12753	3744	0	540664	0	0	667	-1339	4526	5935	60044	-70028
D13T15	2356	1988	0	119678	0	0	273	-4210	5047	10119	13147	-109270
D16	1032	579	0	4571	0	0	350	309	37	12	5142	-10652
D17T18	19309	9367	0	131614	14	889	31679	212	72	290	69539	-27287
D19	9812	6374	0	303870	0	0	253	-3006	2166	3870	115382	-91464
D20T21	43995	6396	0	236683	0	0	4861	-953	2834	4566	169942	-168073
D22	11112	5639	0	36419	0	0	967	663	116	149	27193	-49318
D23	3083	1088	0	11683	0	0	676	455	32	50	9184	-15810
D24	351	2219	0	3329	0	0	614	8345	65	58	41455	-102413
D25	2630	6237	0	19723	5	0	7337	3980	153	107	34408	-43417
D28	2935	13495	0	20619	0	0	34629	16725	1591	2732	132958	-159568
D26	6314	6984	0	103029	1	0	128147	8571	2420	7713	186485	-366193
D27	1052	2496	0	38726	0	0	31876	2871	129	98	40395	-86280
D29	2197	17265	0	220664	0	0	87752	3642	124	486	102973	-198522
D30	1286	1208	0	15715	0	0	83755	2415	52	51	93439	-39042
D31T33	21682	2403	0	122256	0	0	14910	2822	3679	7654	30761	-91278
D35T39	6660	4082	0	177841	1	1445	1671	-101	134	30	1341	-2868
D41T43	1862	3443	0	230	0	0	715189	-471	154	0	3310	-2883
D45T47	56331	30042	0	1070982	8938	190	86817	3579	7891	11544	169874	-294639
D55T56	15659	4378	0	546886	1984	0	1126	-10	37799	38238	1203	-39217
D49T53	18042	12013	0	188708	125	0	11331	763	38303	48025	99672	-87577
D61	21003	9493	0	365630	156	0	14721	-60	48	187	13664	-9725
D64T66	107038	41235	0	1033380	0	0	3816	-268	114	147	112771	-141715
D68	39984	49367	0	1551068	6	0	8164	-49	5303	5759	3500	-7527
C71	7079	3857	0	32721	66	2	92	-17	7421	6953	37157	-15438
D62T63	17037	7942	0	26429	24	1044	91094	-136	70	33	15522	-30907
D69T82	142683	56949	0	189429	83	6	330682	-557	287	26	133097	-73560
D84	12673	6123	0	261420	17433	1828166	20162	-137	484	3038	10245	-2277
D85	7035	3804	0	151986	12441	761725	16364	-35	3063	5977	5531	-3471
D86T88	18400	557	0	1542063	183282	0	2280	-31	3139	306	2403	-3474
D90T96	24484	35068	0	550220	67149	1138	2379	-135	12367	11440	22574	-21959
D97T898	0	0	0	15648	0	0	0	0	0	0	0	0
TXS_INT_FNL: Taxes less subsidies on intermediate and final products	551	339	0	529744	0	0	0	0	0	13266	0	0
TTL_INT_FNL: Total intermediate and final expenditure at purchasers' prices	690617	359590	0	10256902	291900	2594603	1745597	33603	139824	189539	1908341	-2662200
VALU: Value added at basic prices	1079482	561402	15648	0	0	0	0	0	0	0	0	0
OUTPUT: Output	1770099	920993	15648	0	0	0	0	0	0	0	0	0

References for Online Appendix

Abrams, M., and Weiss, J. 2008. *Malicious control system cyber security attack case study - Maroochy Water Services, Australia*, McLean, VA: The MITRE Corporation.

Amoroso, E. G. 1994. *Fundamentals of Computer Security Technology*, *Upper Saddle River, NJ: Prentice-Hall.*

Applegate, S. D., and Stavrou, A. 2013. "Towards a cyber conflict taxonomy," in *2013 5th International conference on Cyber Conflict*, *IEEE*, pp. 1-18.

Armerding, T. 2018. "SamSam ransomware keeps striking - victims still unprepared" (https://www.synopsys.com/blogs/software-security/samsam-ransomware/; accessed April 20, 2021).

Armington, P. S. 1969. "A theory of demand for products distinguished by place of production," *Staff Papers* (16:1), pp. 159-178.

Avelino, A. F. T., and Hewings G. J. D. 2017. "The challenge of estimating the impact of disasters: many approaches, many limitations and a compromise" (http://www.real.illinois.edu/d-paper/17/17-T-1.pdf; accessed April 20, 2021).

Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., and Williams, J. 2017. "Contagion in cyber security attacks," *Journal of the Operational Research Society* (68:7), pp. 780-791.

Ballard, C. L., and Johnson, M. 2017. "Applied General Equilibrium Analysis: Birth, Growth, and Maturity," *History of Political Economy* (49:Supplement), pp. 78-102.

Berg, M., Hartley, B., and Richters, O. 2015. "A stock-flow consistent input-output model with applications to energy price shocks, interest rates, and heat emissions," *New Journal of Physics* (17:1), 015011. doi:10.1088/1367-2630/17/1/015011

Bhattarai, K., Haughton, J., Head, M., and Tuerck, D. G. 2017. "Simulating corporate income tax reform proposals with a dynamic CGE model," *International Journal of Economics and Finance* (9:5), pp. 20-35. doi:10.5539/ijef.v9n5p20

Biener, C., Eling, M., and Wirfs, J. H. 2015. "Insurability of cyber risk: an empirical analysis," *The Geneva Papers on Risk and Insurance - Issues and Practice* (40:1), pp. 131-158. doi:10.2139/ssrn.2577286

Bishop, M. 1995. "*A taxonomy of UNIX system and network vulnerabilities (University of California at Davis No. Report CSE-95-10)*," (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.33.5712; accessed April 20, 2021).

Bollen, J. 2015. "The value of air pollution co-benefits of climate policies: analysis with a global sector-trade CGE model called WorldScan," *Technological Forecasting and Social Change* (90), pp. 178-191. doi:10.1016/j.techfore.2014.10.008

Börjeson, L., Höjer, M., Dreborg, K. H., Ekvall, T., and Finnveden, G. 2006. "Scenario types and techniques: towards a user's guide," *Futures* (38:7), pp. 723-739. doi:10.1016/j.futures.2005.12.002

Boteler, D. H., Pirjola, R. J., and Nevanlinna, H. 1998. "The effects of geomagnetic disturbances on electrical systems at the Earth's surface," *Advances in Space Research* (22:1), pp. 17-27. doi:10.1016/s0273-1177(97)01096-x

Bounfour, A., Dieye, R., Kammoun, N., and Ozaygen, A. 2018. "Macro estimates of intangibles cyber-risks," (https://www.hermeneut.eu/wp-content/uploads/2018/08/HERMENEUT-D3.2-Macro-estimates-of-intangibles-cyber-risks.pdf; accessed April 20, 2021).

Brandom, R. 2017. "UK hospitals hit with massive ransomware attack: sixteen hospitals shut down as a result of the attack," (https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/; accessed April 20, 2021).

Cebula, J. J., Popeck, M. E., and Young, L. R. 2014. "A Taxonomy of Operational Cyber Security Risks Version 2" (https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf, doi:10.21236/ada609863)

Dejung, S. 2017. “Economic impact of cyber accumulation scenarios,” Swiss Insurance Association Cyber Working Group.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J., and Winkelman, Z. 2018. “Estimating the global cost of cyber risk: methodology and examples”. doi:10.7249/rr2299 (https://www.rand.org/pubs/research_reports/RR2299.html; accessed April 20, 2021).

Durance, P., and Godet, M. 2010. “Scenario building: uses and abuses,” *Technological Forecasting and Social Change* (77:9), pp. 1488-1492. doi:10.1016/j.techfore.2010.06.007

Eling, M., and Schnell, W. 2016. “What do we know about cyber risk and cyber risk insurance?,” *The Journal of Risk Finance* (17:5), pp. 474-491. doi:10.1108/jrf-09-2016-0122

European Union Agency for Network and Information Security. 2018. “ENISA threat landscape report 2017” (https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017; accessed April 20, 2021).

Falco, G., Viswanathan, A., Caldera, C., and Shrobe, H. 2018. “A master attack methodology for an AI-based automated attack planner for smart cities,” *IEEE Access* (6), pp. 48360-48373. doi:10.1109/access.2018.2867556

Feenstra, R. C., and Sasahara, A. 2018. “The “China shock,” exports and U.S. employment: a global input-output analysis,” *Review of International Economics* (26:5), pp. 1053-1083. doi:10.1111/roie.12370

Guevara, Z., and Domingos, T. 2017. “The multi-factor energy input-output model,” *Energy Economics* (61), pp. 261-269. doi:10.1016/j.eneco.2016.11.020

Hallegatte, S. 2008. “An adaptive regional input-output model and its application to the assessment of the economic cost of Katrina,” *Risk Analysis* (28:3), pp. 779-799. doi:10.1111/j.1539-6924.2008.01046.x

Hansman, S., and Hunt, R. 2005. “A taxonomy of network and computer attacks,” *Computers & Security* (24:1), pp. 31-43. doi:10.1016/j.cose.2004.06.011

Howard, J. D. 1997. “An analysis of security incidents on the Internet,” PhD thesis, Carnegie Mellon University (https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52454; accessed April 20, 2021).

Howard, J. D. 2015. “Using a common language for computer security incident information,” in *Computer Security Handbook*, S. Bosworth, M. E. Kabay, and E. Whyne (eds.). Hoboken, NJ: John Wiley & Sons, pp. 8.1-8.21. doi:10.1002/9781118851678.ch8

Institute and Faculty of Actuaries. 2018. “Cyber operational risk scenarios for insurance companies: research project,” (https://www.actuaries.org.uk/news-and-insights/news/ifoa-publish-cyber-operational-risk-scenarios-insurance-companies; accessed April 20, 2021).

Jin, X., Shi, X., Gao, J., Xu, T., and Yin, K. 2018. “Evaluation of loss due to storm surge disasters in China based on econometric model groups,” *International Journal of Environmental Research and Public Health* (15:4), 604. doi:10.3390/ijerph15040604

Kajitani, Y., and Tatano, H. 2018. “Applicability of a spatial computable general equilibrium model to assess the short-term economic impact of natural disasters,” *Economic Systems Research* (30:3), pp. 289-312. doi:10.1080/09535314.2017.1369010

Koks, E. E., and Thissen, M. 2016. “A multiregional impact assessment model for disaster analysis,” *Economic Systems Research* (28:4), pp. 429-449. doi:10.1080/09535314.2016.1232701

Koks, E. E., Carrera, L., Jonkeren, O., Aerts, J. C. J. H., Husby, T. G., Thissen, M., Standardi, G., and Mysiak, J. 2015. “Regional disaster impact analysis: comparing input-output and computable general equilibrium models,” *Natural Hazards and Earth System Sciences Discussions* (3:11), pp. 7053-7088. doi:10.5194/nhessd-3-7053-2015

Langarita, R., Duarte, R., Hewings, G., and Sánchez-Chóliz, J. 2019. “Testing European goals for the Spanish electricity system using a disaggregated CGE model,” *Energy* (179), pp. 1288-1301. doi:10.1016/j.energy.2019.04.175

Lin, J., Tai, K., Tiong, R. L. K., and Sim, M. S. 2016. "A general framework for critical infrastructure interdependencies modeling using economic input-output model and network analysis," in *Complex Systems Design & Management Asia*, Cardin, M.-A., Fong, S., Krob, D., Lui, P. and Tan, Y. (eds.). Cham: Springer, pp. 59-74. doi:10.1007/978-3-319-29643-2_5

Lloyd's. 2015. "Business blackout: the insurance implications of a cyber attack on the US power grid," (https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout; accessed April 20, 2021).

Mahmoud, M., Liu, Y., Hartmann, H., Stewart, S., Wagener, T., Semmens, D., Stewart, R., Gupta, H., Dominguez, D., Dominguez, F., Hulse, D., Letcher, R., Rashleigh, B., Smith, C., Street, R., Ticehurst, J., Twery, M., van Delden, H., Waldick, R., White, D., and Winter, L. 2009. "A formal framework for scenario development in support of environmental decision-making," *Environmental Modelling & Software* (24:7), pp. 798-808. doi:10.1016/j.envsoft.2008.11.010

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., and Yautsiukhin, A. 2017. "Cyber-insurance survey," *Computer Science Review* (24), pp. 35-61. doi:10.1016/j.cosrev.2017.01.001

Menoni, S., Bonadonna, C., García-Fernández, M., and Schwarze, R. 2017. "Recording disaster losses for improving risk modelling capacities," in *Science for disaster risk management 2017: knowing better and losing less*, K. Poljanšek, M. Main Ferrer, T. de Groeve, and I. Clark (eds.). Luxembourg: Publications Office of the European Union, pp. 83-97. doi:10.2788/842809

Miller, M., Liu, L., Shwiff, S., and Shwiff, S. 2018. "Macroeconomic impact of foot-and-mouth disease vaccination strategies for an outbreak in the Midwestern United States: A computable general equilibrium," *Transboundary and Emerging Diseases* (66:1), pp. 156-165. doi:10.1111/tbed.12995

Nakamura, S., and Kondo, Y. 2018. "Toward an integrated model of the circular economy: Dynamic waste input-output," *Resources, Conservation and Recycling* (139), pp. 326-332. doi:10.1016/j.resconrec.2018.07.016

Nakicenovic, N., and Swart, R. 2000. Special Report on Emissions Scenarios. Working Group III, Intergovernment Panel on Climate Change (IPCC), Vol. 1.

National Association of Insurance Commissioners. 2019. "Data, innovation & cyber" (https://www.naic.org/cipr_topics/topic_cyber_risk.htm; accessed April 20, 2021).

Niknejad, D. 2019. "Salesforce customers lose CRM data in 20 hour outage" (https://www.cmswire.com/customer-experience/salesforce-customers-lose-crm-data-in-20-hour-outage/; accessed April 20, 2021).

Niknejad, A., and Petrovic, D. 2016. "A fuzzy dynamic inoperability input-output model for strategic risk management in global production networks," *International Journal of Production Economics* (179), pp. 44-58. doi:10.1016/j.ijpe.2016.05.017

Njoya, E. T., and Seetaram, N. 2017. "Tourism contribution to poverty alleviation in Kenya: a dynamic computable general equilibrium analysis," *Journal of Travel Research* (57:4), pp. 513-524. doi:10.1177/0047287517700317

OECD, 2018. "Input-output tables (IOTs)" (http://www.oecd.org/sti/ind/input-outputtables.htm; accessed April 20, 2021).

Öğüt, H., Raghunathan, S., and Menon, N. 2011. "Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection," *Risk Analysis: An International Journal* (31:3), pp. 497-512.

Okon, E. O. 2018. "Natural disasters in Nigeria: an econometric model," *American Journal of Social Science Research* (2:1), pp. 81-101.

Okuyama, Y. 2007. "Economic modeling for disaster impact analysis: past, present, and future," *Economic Systems Research* (19:2), pp. 115-124. doi:10.1080/09535310701328435

Pescaroli, G., and Alexander, D. 2016. "Critical infrastructure, panarchies and the vulnerability paths of cascading disasters," *Natural Hazards* (82:1), pp. 175-192. doi:10.1007/s11069-016-2186-3

Peterson, G. D., Cumming, G. S., and Carpenter, S. R. 2003. "Scenario planning: a tool for conservation in an uncertain world," *Conservation Biology* (17:2), pp. 358-366. doi:10.1046/j.1523-1739.2003.01491.x

Piermantini, R., and Teh, R. 2005. "Demystifying Modeling Methods for Trade Policy," *WTO Discussion Papers*, No. 10. Geneva: WTO.

Poledna, S., Hochrainer-Stigler, S., Miess, M. G., Klimek, P., Schmelzer, S., Sorger, J., Shchekinova, E., Rovenskaya, E., Linnerooth-Bayer, J., Dieckmann, U., and Thurner, S. 2018. "When does a disaster become a systemic event? Estimating indirect economic losses from natural disasters," *arXiv preprint* (https://arxiv.org/abs/1801.09740; accessed April 20, 2021).

Richardson, R., and North, M. M. 2017. "Ransomware: evolution, mitigation and prevention," *International Management Review* (13:1), pp. 10-21.

Risk Management Solutions Inc. 2016. "Managing cyber insurance accumulation risk" (https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf; accessed April 20, 2021).

Romanosky, S. 2016. "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity* (2:2), pp. 121-135. doi:10.1093/cybsec/tyw001

Rose, A. 2004. Economic principles, issues, and research priorities in hazard loss estimation. in *Modeling Spatial and Economic Impacts of Disasters*, Y. Okuyama and S. E. Chang (eds.). New York: Springer, pp. 13-36.

Rose, A., Sue Wing, I., Wei, D., and Wein, A. 2016. "Economic impacts of a California tsunami," *Natural Hazards Review* (17:2), 04016002. doi:10.1061/(asce)nh.1527-6996.0000212

Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B., and Ralph, D. 2014. "Stress test scenario: sybil logic bomb cyber catastrophe," *Cambridge Risk Framework series, Centre for Risk Studies, University of Cambridge*.

Sahin, I., and Yavuz, O. 2015. "Econometric analysis of natural disasters' macro-economic impacts: an analysis on selected four OECD countries," *Journal of Business, Economics and Finance* (4:3), pp. 430-442. doi:10.17261/Pressacademia.2015313064.

Saldaña-Zorrilla, S. O., and Sandberg, K. 2009. "Spatial econometric model of natural disaster impacts on human migration in vulnerable regions of Mexico," *Disasters* (33:4), pp. 591-607. doi:10.1111/j.1467-7717.2008.01089.x

Santos, J. R., and Haimes, Y. Y. 2004. "Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures," *Risk Analysis* (24:6), pp. 1437-1451. doi:10.1111/j.0272-4332.2004.00540.x

Teoh, T. T., Nguwi, Y. Y., Elovici, Y., Ng, W. L., and Thiang, S. Y. 2018. "Analyst intuition inspired neural network based cyber security anomaly detection," *International Journal of Innovative Computing Information and Control* (14:1), pp. 379-386.

Trautman, L. J., and Ormerod, P. 2018. "Wannacry, ransomware, and the emerging threat to corporations," *SSRN Electronic Journal*. doi:10.2139/ssrn.3238293

van Notten, P. W. F., Rotmans, J., van Asselt, M. B. A., and Rothman, D. S. 2003. "An updated scenario typology," *Futures* (35:5), pp. 423-443. doi:10.1016/s0016-3287(02)00090-3

Wang, S. S. 2019. "Integrated framework for information security investment and cyber insurance," *Pacific-Basin Finance Journal* (57), in press. doi:10.1016/j.pacfin.2019.101173

Wei, F., Koc, E., Soibelman, L., and Li, N. 2018. "Disturbances to urban mobility and comprehensive estimation of economic losses," *Polytechnica* (1:1-2), pp. 48-60. doi:10.1007/s41050-018-0005-1

West, G. R. 1995. “Comparison of Input-Output, Input-Output + Econometric and Computable General Equilibrium Impact Models at the Regional Level,” *Economic Systems Research* (7:2), pp. 209-227. doi:10.1080/09535319500000021

World Economic Forum. 2014. “Global risks 2014 - ninth edition” (http://reports.weforum.org/global-risks-2014/?doing_wp_cron=1548774994.0724980831146240234375; accessed April 20, 2021).

Yadav, T., and Rao, A. M. 2015. “Technical aspects of cyber kill chain,” *Security in Computing and Communications*, Cham: Springer International Publishing Switzerland, pp. 438-452. doi:10.1007/978-3-319-22915-7_40

Zhang, W., Yang, J., Zhang, Z., and Shackman, J. D. 2017. “Natural gas price effects in China based on the CGE model,” *Journal of Cleaner Production* (147), pp. 497-505. doi:10.1016/j.jclepro.2017.01.109

Zio, E. 2016. “Challenges in the vulnerability and risk analysis of critical infrastructures,” *Reliability Engineering & System Safety* (152), pp. 137-150. doi:10.1016/j.ress.2016.02.009