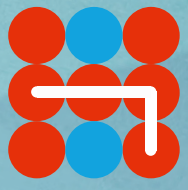
COI VULNERABILITIES AND RESILIENCE

Hybrid CoE Working Paper 4

NOVEMBER 2019

Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?

JUKKA SAVOLAINEN



Hybrid CoE

Hybrid CoE Working Paper 4

Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?

JUKKA SAVOLAINEN

Hybrid CoE Working Papers are medium-length papers covering work in progress. The aim of these publications is to share ideas and thoughts, as well as to present an analysis of events that are important from the point of view of hybrid threats. Some papers issue recommendations. They cover a wide range of important topics relating to our constantly evolving security environment. Working papers are not peer reviewed.

The Vulnerabilities and Resilience COI focuses on understanding member states' and institutions' vulnerabilities and improving their resilience by sharing best practices, developing new policy proposals and identifying topics to be studied further. The aim of the COI is also to improve public-private and civil-military partnership in countering hybrid threats.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-27-4
ISSN 2670-160X

Second version of the publication. Previously published as "Working Paper: Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure ġWeapons of Mass Disturbance (WMDi)?"

November 2019

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Summary

The text takes stock of Critical Infrastructure-related lessons identified and learned during a two-year assessment done by the Community of Interest for Vulnerabilities and Resilience in the European Centre of Excellence for Countering Hybrid Threats. Modern Critical Infrastructure seemingly serves as an effective instrument in the hands of adversaries able and willing to use hybrid tools. No widespread use of this *possibility* has thus far been tested in any serious conflict between developed states. The first time will quite likely surprise many.

Reference is made to modern Critical Infrastructure Risk theory, which is connected to escalation theory of International conflicts. According to the main finding, a hybrid adversary may gain significant benefits in conflicts by acting against Critical Infrastructure in countries that are dependent on an open market economy and a transparent democratic decision-making process. *Distraction* and *disruption* describe the extreme tones of such an effect. Available asymmetric techniques such as cyber tools, covert special operations, information operations, political agitation and economic instruments, when combined with the vulnerabilities of modern Critical Infrastructure, form a new threat. It is suggested that this threat be named *"Weapons of Mass Disturbance (WMDi)"*.

Resilience, attribution and exchange of information remain key words when improving defences against such potential activity.

Relevant Critical Infrastructure is mainly owned by companies, not public services. The way forward must be planned together between states and the private sector. Community-level responses (EU, NATO) would be desirable in terms of regulation as well as preparedness.

Foreword

Two years have elapsed since the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) got started in Helsinki. During that time, its Community of Interest for "Vulnerabilities and Resilience" (COI VR) has had many good opportunities to meet with numerous people from various governments and organisations, participate and contribute to several events concerning hybrid threats, and conduct some indigenous studies as well. Especially, it has organised a few working strands taking stock of what might be the key vulnerabilities and how to improve resilience in the respective fields. These working strands have been named as follows: "Legal resilience", "Harbor protection", "Sea Lines of Communication", "Drones", "Hybrid Threats and Energy Sector", "EU-NATO cooperation in Civil Protection" and "Hybrid and Finance". All strands have consisted of more than just one event (finance, where a kick-start meeting has only been organised thus far).

This selection of topics was aimed at augmenting the mainstream discussion around Hybrid Threats, where disinformation, media, elections and, more generally, societal issues are well covered. COI VR tried to look closely at the technologies and interlinked services that feed and maintain our current way of life. This mainly refers to functionalities that are called "Critical Infrastructure" by the EU[1] and "Civil Preparedness"[2] by NATO.

We are grateful to the contributing partners and the several hundred participants who joined these events. Now, it is time to take stock of what we learned and produce a structural model based on the key findings. This will hopefully stimulate further work that needs to be done.

To that end, we introduce the technological concept of "Resilience" and link it with conflicts as a potential vector of influence. What we find is a new constellation that perhaps deserves to be named "Weapons of Mass Disturbance, WMDi".

1 Council Directive 2008/114/EC: EU Critical Infrastructure is an "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".
2 NATO Press Release (2016) 118/8th July 2016: "We will protect our populations and territory by strengthening continuity of government, continuity of essential services and security of critical civilian infrastructure; and we will work to ensure that our national and NATO military forces can at all times be adequately supported with civilian resources, including energy, transportation, and communications."

Hybrid Threats

In the context of HybridCoE, Hybrid Threats are regarded as actions targeting democratic states' decision-making processes while hurting or undermining the target. The activities may utilise any sort of vulnerabilities in any domains found exploitable by adversaries. Their magnitude may vary along the axis influencing – operations – hybrid warfare. Often, it is in an adversary's interest to keep its action below such thresholds that would provoke countermeasures. The key thresholds are detection, attribution and war. If one does not detect the type of malicious activity that is being targeted, one will not respond. If one detects it but cannot prove or even know who caused it (missing attribution), one will not respond. If one knows what was done and by whom, but the harmful or even dangerous or devastating activity remains under the threshold of International armed conflict, one can, even still, hardly respond by military means.[3]

3 For more on the concept and its description, see www.hybridcoe.fi

Critical Infrastructure as a target for hybrid threats – Lessons learned in the workstrands

Modern Critical Infrastructure[4] seemingly serves as an effective instrument in the hands of adversaries able and willing to use hybrid tools. No widespread use of this possibility has thus far been tested in any serious conflict between developed states. The first time will quite likely surprise many.[5] What, then, has changed since WWII and the Cold War era?

JIT deliveries supported by IT through global markets

The main relevant drivers of change have been the new information technologies, open market economy and globalised markets. All have led to an unforeseen increase in efficiency, producing in turn not just steady growth in the global and regional economies of the Western Hemisphere, but in most other parts of the globe as well. Besides growth in volumes, this system has produced an increased reliability on deliveries. If one part of a chain somewhere fails, another supplier or route will normally be found soon thereafter. Thus, one has all the necessary goods readily available, and does not need to know how they arrived at the local market or doorstep.

A significant feature has also been the reduction of storage systems and shift towards "Just In Time" (JIT) deliveries. Almost all ready-made products loose value by getting older every day; capital is invested in them, and besides, the storing of products is an extra cost. This all suggests that products should be delivered as soon as possible from the factory to the end-user. Any interim storage is avoided as much as possible.

The swiftness of deliveries is nowadays strongly supported by IT applications. Digitalisation of the entire logistic chain and its coexisting communities is an ongoing megatrend. At this time, the control of deliveries through major seaports would hardly be possible by manual means alone.

Digital payments and asset management

The development of such a swift economy required a swift financial system on its side. This has now been achieved. Cash has almost become obsolete as a means of making payments in business, and likewise salaries, social benefits, interests, taxes or anything aside from minor local transactions have gone digital. Financial assets also exist mainly as digits on servers only.

Critical Infrastructure Interdependencies

Societies are dependent on the smooth functioning of large and interdependent Critical Infrastructure systems. Only a few houses and smaller flats can be properly heated by their own in-house systems. Preferably, they have been connected to a district heating system. Besides district heating, many other systems (distribution of fuels, fresh water, sewage) are dependent on the availability of electricity, as they all depend on pumps. Communication systems require electricity for

4 The concept of "Critical Infrastructure" shall here be used in its broadest sense, covering infrastructure such as factories, hospitals, power plants, electric grid, airports, ports, bridges and roads, but also logistics chains as well as networks that produce and transfer information, goods and money, i.e. all large physical or virtual systems that provide modern societies with what they need for normal daily life. It must be recognised that formal definitions do exist and they may in part have a different scope. For example, the EU so far does not recognise the finance sector as a part of Critical Infrastructure and NATO has defined this very same topic under the term "Civil Preparedness". These finesses are not in the scope of this paper and have to be left aside for now. This will in no way cause prejudice in using any authorised or generally approved definitions in HybridCoE's further work.
5 The ongoing conflict in Ukraine should, at any rate, be seen as a test platform based on the use of destructive cyber tools (Petya and Not-Petya malwares).

the transmission of data. The failure to generate or distribute electricity will lead to multiple failures elsewhere.

Critical Infrastructure is now largely privately owned

Previously, the investment in and maintenance of Critical Infrastructure as well as preparedness of critical deliveries were regarded as something that states or the public sector in general should take care of, and this led to the creation of various publicly owned companies. This has now changed; especially since the end of the Cold War, Western governments have reduced their hold on these assets. Examples of such a shift within the course of a few decades include power generation companies, the power grid, telecommunication companies, communication networks, national aviation companies, airports and airfields, maritime ports and even many services that were previously state-run services, such as mail service, road construction, fairways and even pilotage at sea. The same goes for health-care services.

From a resilience standpoint, current Western open-market systems contain some obvious vulnerabilities. These are as follows:

1. Based on the JIT delivery concept, the stock of all goods has been reduced on purpose. In the case of a major disruption of market-guided logistical systems, reserves near the user end would be scarce.

2. Globalisation means longer delivery distances for many goods. Few countries are any longer self-sustaining in terms of supplying goods to ensure a basic standard of living (food, medicine, clothes, fuel).

3. Digital systems have already become dominant in large parts of the logistical system. If the IT systems fail, the goods will be lost. This makes logistics a feasible target for a cyberattack.[6]

4. Finance systems are also vulnerable to cyber-attacks. If payments cannot be made, goods will not move. If goods do not move, there will soon be a lack of food and other daily necessities.

5. All logistics and finance are based on telecommunications. Telecommunication systems are vulnerable to cyberattacks, but they can also be effectively paralysed physically by hitting the main congestion points. While it will always be possible to recover from physical damage, it will take time.

6. Societies are dependent on the proper functioning of large and interdependent Critical Infrastructure systems (electricity, water, sewage, heating, mass communication and information). Like telecommunications, these systems can also be damaged by cyber or physical means.

7. The systems are based on the market economy (as they should be), and companies are all the time looking for lean solutions to avoid costs. Being prepared for such extreme crisis scenarios, which have not been witnessed earlier, cannot be favoured as a solution.

8. The public sector can exercise no direct command or control over CI companies in normal situations.[7]

9. National actors cannot easily remedy problems that arise abroad. A serious international market disturbance may lead to congestion with deliveries and financing. Such events may cause serious damage wherever such goods no longer arrive (as they are no longer produced locally).

10. In an open society, technical information on CI systems is easily available.

11. Systemic and/or market disruptions may rapidly lead to severe political consequences.

6 The global logistics company Maersk has publicly announced that it suffered serious losses because of the Not-Petya malware that spread throughout Ukraine in 2017.
7 Nevertheless, interventions are commonly used and may be based on regulations or the public funding of various preparedness measures.

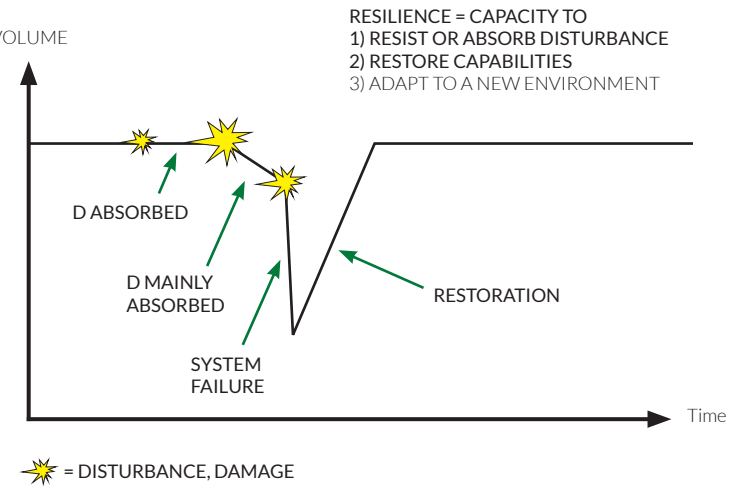
Claims 1–11 above are relevant everywhere. Nevertheless, countries with authoritarian regimes are in many cases less vulnerable. This results from the stronger position of the political leadership with regard to the private sector as well as public opinion and political processes. This advantage is even stronger wherever such governments have successfully improved their domestic livelihood production and CI architecture such that they are more self-sustaining. This disparity may provide some authoritarian rulers with a significant comparative advantage in conflicts with the West.

Based on what has been stated above, one must have due concern regarding the resilience of inter-dependent local and global Critical Infrastructure systems.

Critical Infrastructure Resilience

PICTURE 1.
CI RESILIENCE

Source: Igor Linkov



Picture 1 above explains the main features of CI resilience. This description is simplified and rather generic, and it covers any type of productive CI system. The idea can most easily be understood by imagining the vertical axis "volume" as showing the electrical power produced for the national grid. The production level at the very start is what is expected for normal daily life. Resilience means, first, the capacity to resist disturbance by absorbing a negative impact entirely or at least partially, and second, the ability to restore capabilities after the damage – the sooner the better. After a few such impacts, near all power may have been lost, but power will be restored by various means in normal cases.[8]

All actors in the field of Critical Infrastructure have developed their own understanding of the threats and risks they are facing. Based on this understanding, they have also factored some level of resilience into their systems. As can be seen in the daily lives of people, such resilience has thus far worked because societies are used to receiving those particular services they need.

The analyses used by CI companies are based on actual field experience and information exchange with colleagues and peers, and they produce a sound assessment of the credible hazards associated with natural disasters, criminals and future hackers, etc. Resilience will be built up accordingly with reasonable costs (as all elements of extra resilience produce costs).

The anticipated man-made intrusions attempt to steal some economic benefits and leave the perpetuators free of judicial consequences. They should remain modest in terms of damage and detectability. In contrast, a hybrid operation may be well prepared (with intelligence and intrusion completed before action) and sufficiently resourced to overwhelm the system's defences and cause devastation. It may be something that, based on normal experience, could not be anticipated. It can also hit not just one vital system at a time, but various systems. In other words, these developments will come from outside the box. The rest of this paper tries to explain why hybrid operations should be regarded as a potential risk linked to international conflicts.

8 If that is not possible, the market shall adapt to a new situation by limiting consumption until new capacity has been achieved.

Critical Infrastructure as a potential instrument in an international conflict

Let us imagine a situation where a geographic area X is under geopolitical speculation. One side (Blue) is securing X's integrity against another side (Red), which is motivated to seize control of the area whenever possible (either by political or military means). The overall power balance in the area is slightly dominated by the Blue side, which has a defensive agenda only: Preserving the status quo.

Picture 2 describes a change in the situation: Red starts building up regional capacity, leading to a shift in the status quo. At one point, Red becomes superior and seems to be promoting growth of its military capabilities. Blue responds by increasing its own capabilities so that the status quo could be resumed (this means Blue should remain slightly superior in that very area).[9]

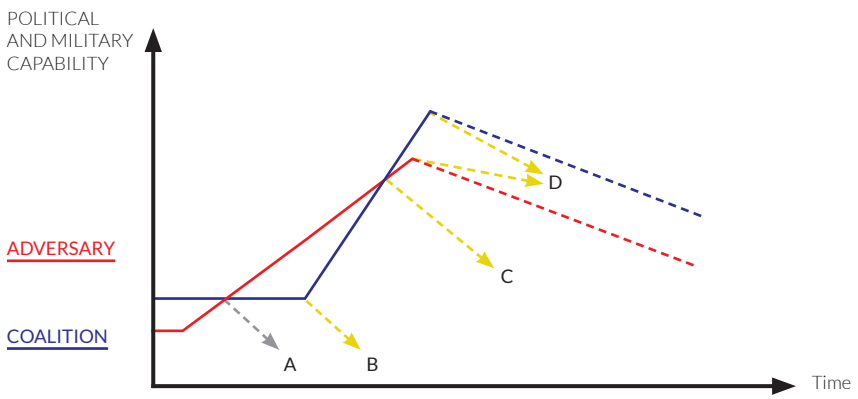
The decisive question in this development is, does the Blue coalition (region X + the supportive states) manage to deter the possible aggression by re-establishing superiority in the region? This takes place between points B and D. Picture 3 focuses on this detail.

The area delimited by the blue box in picture 3 is now projected on a slightly different scale in picture 4. It shows only the time frame when the Blue coalition is supposed to strengthen its capabilities over those of the Red coalition – soon enough to prevent a military escalation.

Now, it is useful to return to what was stated earlier about the vulnerabilities of Critical Infrastructure: it can be damaged by various means, and the outcome may be devastating and have serious

PICTURE 2.
COALITION RESPONSE CAPABILITY BUILDING DURING AN EMERGING CRISIS

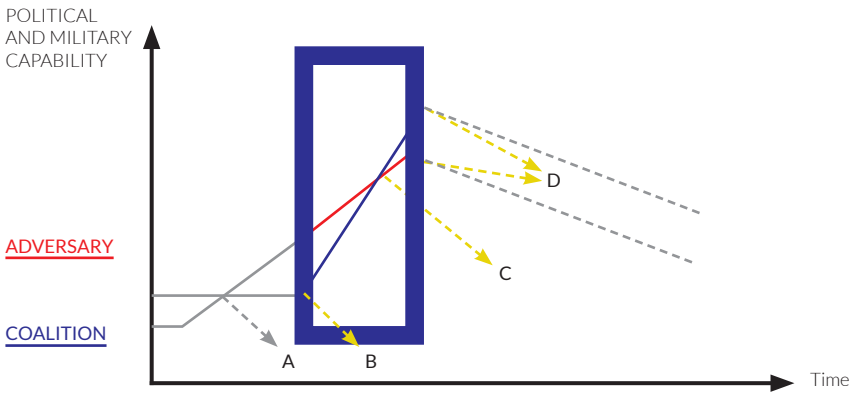
Source: Peter Billing



A = ADVERSARY'S CAPABILITY EXCEEDS COALITION'S CAPABILITY – RISKS RISE
B = COALITION STARTS EXPANDING ITS CAPABILITY
C = ADVERSARY LOSES ITS ADVANTAGE; NO MORE INTERESTED TO USE MILITARY OPTION
D = POINT, WHERE THE CAPABILITY REDUCTION CAN START SAFELY, IF RETURN POSSIBLE

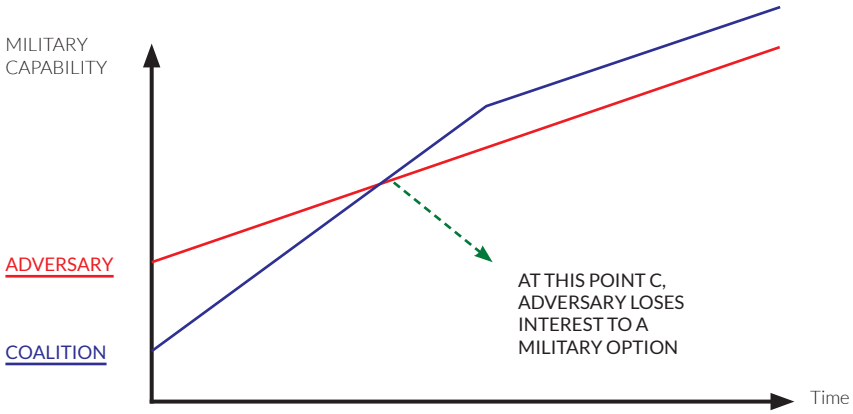
9 Peter Billing, *Eskalation und Deeskalation internationaler Konflikte. Ein Konfliktmodell auf der Grundlage der empirischen Auswertung von 288 internationalen Konflikten seit 1945* (Frankfurt: Lang Verlag, 1992).

PICTURE 3.
BETWEEN PHASES B AND D, C IS THE DECISIVE POINT



A = ADVERSARY'S CAPABILITY EXCEEDS COALITION'S CAPABILITY – RISKS RISE
B = COALITION STARTS EXPANDING ITS CAPABILITY
C = ADVERSARY LOSES ITS ADVANTAGE; NO MORE INTERESTED TO USE MILITARY OPTION
D = POINT, WHERE THE CAPABILITY REDUCTION CAN START SAFELY, IF RETURN POSSIBLE

PICTURE 4.
INCREASING OF COALITION RESPONSE CAPABILITY IN ORDER TO PREVENT ADVERSARY FROM USING A MILITARY ADVANTAGE



market-related and political consequences. Additionally: 1) an ongoing serious disturbance would, at least in the short term, weaken any country's decision-making capacity; 2) the logistics of a military force always is to some extent dependent on civilian markets and society – nowadays even more so than a few decades ago. Thus, sudden peace-time damage to current market supply chains would reduce the capacity of military logistics. This would in turn reduce the available potential range of activities.[10]

Counter CI hybrid operation attributable to the adversary

Picture 5 describes a situation wherein the Blue side is suddenly hit by a serious hybrid operation targeting major parts of its Critical Infrastructure. Such a disturbance would limit the decision-making and military capability of the Blue side. In the picture, the Critical Infrastructure resilience curve has been merged with picture 4, where Blue was preparing to overrun the regional power of Red.

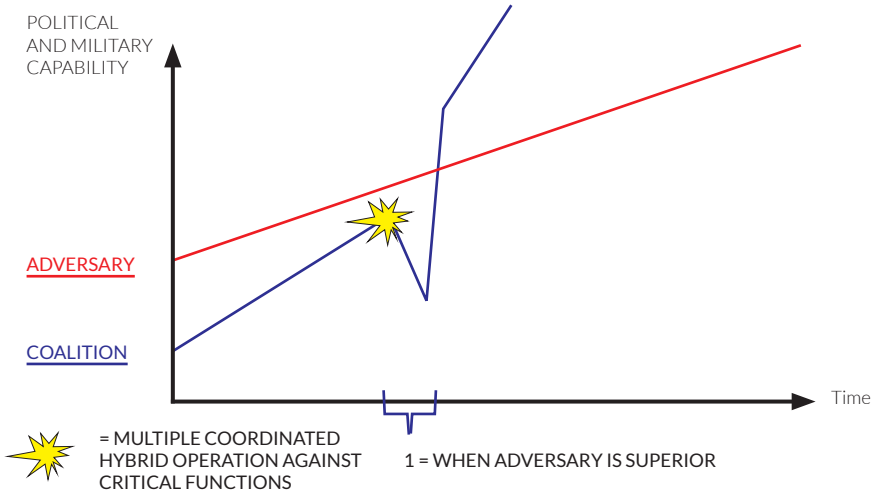
In this basic case, the CI disturbance would have a short-term effect only. The systems would be resumed soon thereafter and the coalition's decision-making capacity as well as its military capabilities would recover rapidly. A significant loss in the coalition's capabilities would take place, but the effect would be only temporary. The time span when the adversary maintains substantial superiority would be short. This can, nevertheless, be harvested by the Red side, which would make a decisive pre-planned move in the target area leading to a "Fait Accompli".

This would be quite likely be the result of a case where the Blue side can make a clear attribution of the hybrid actor. If it could conclude that the events were inflicted by the Red side for the sole purpose of damaging the Blue coalition, it would likely boost its level of preparedness quite soon. It would also likely remain in a revanchist mode even after having recovered from the attack.

Counter CI hybrid operation and no attribution

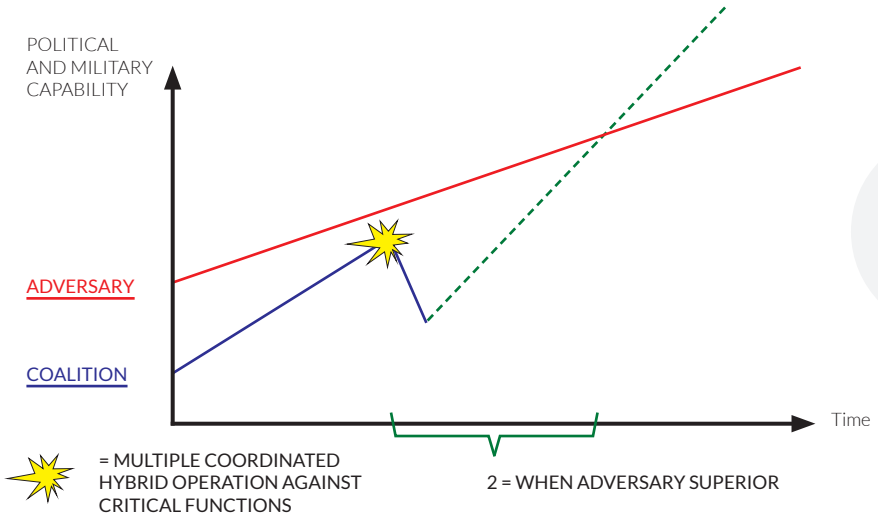
In another case, the attribution cannot be made clearly. If so, societies are likely to first pay attention to their internal problems and strengthening of the Blue coalition would remain as a secondary priority in national politics. This would, nevertheless, allow for the successful mid-term building of coalition capability, as shown in picture 6.

PICTURE 5.
RAPID RECOVERY AND BOOST AFTER A CIS DAMAGE



10 These reductions in military logistic capacity would take place immediately and have at least a short-term impact. This impact would lose its substance if societies were mobilised to handle a military conflict as their ongoing main threat ("all-out war"). This kind of mobilisation has not been seen in the Western world since WWII.

PICTURE 6.
NORMAL RECOVERY AND BOOST AFTER A CIS DAMAGE



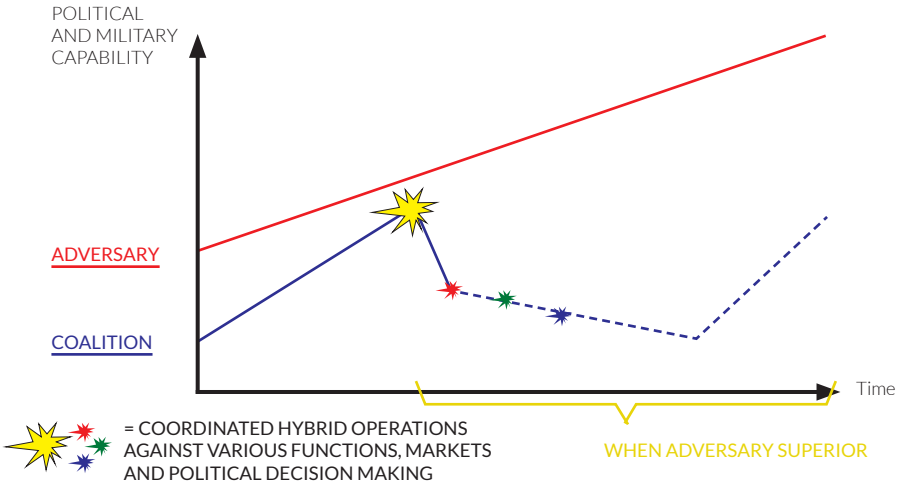
Lacking attribution of the cause behind problems will allow the Red side to remain superior for a longer time. This advantage can perhaps be utilised by the Red side in operations or political manoeuvres. The risk for revanchist behaviour on the part of the Blue after the developments is lower than if the attribution was strong.

Counter CI operation enforced by a divisive hybrid campaign

A more serious development ensues after a hybrid operation in which attribution is not clear, and in addition to direct and indirect damages, the operations lead to a division of the coalition. The adversary might reach this outcome by augmenting the main operation with additional measures in other fields. This would be the case if citizens in some of the coalition countries could be led to believe that the CI damage originated with an ally. This would make the coalition-building effort far more difficult, and it would take a long time to resume capabilities.

This would allow for a military solution or a political arrangement only, leading to the desired outcome from the Red perspective. With the failure of Blue to demonstrate decisive support, the threatened nations might be tempted to adjust to a new status quo and avoid military conflict with the Red side.[11] If attribution remains unclear, even after such developments, it would be difficult to make the argument for revanchist policies in Blue's democratically governed societies.

PICTURE 7.
NO RECOVERY IN SHORT TERM BECAUSE OF MULTIPLE DISRUPTION IN TECHNOLOGY SYSTEMS AND MARKETS



11 According to Sun Tzu, the best sort of victories are those where the outcome is achieved without any battle.

Weapons of Mass Disturbance, WMDi?

Coordinated hybrid operations waged partially through Critical Infrastructure may strongly affect the target countries and their political and military capabilities. Damage can be inflicted through asymmetric means combining cyber tools, well-targeted special operations, the use of disinformation and political agitation.

In the preferred choice from the attacker's (Red) point of view, this occurs without being clearly attributed to the events, and the events would lead to division within the targeted coalition. All benefits would be gained, and no countermeasures (military or political) from the Blue side would follow. This was the case in the last example above.

Even if attribution is successful in the case of an adversary, it is quite possible for the Red side to gain a great deal. If the primary gains of Red (and losses of Blue) at the target area are not vital, the Blue side would not be willing to regard the hybrid operations as immediate acts of war. This would leave the Blue side in a situation where it would start accommodating itself to a new negotiated reality after the Red side had gained its political and military goals in the target area. Nevertheless, the Blue side could remain in a revanchist position.

When the aim is not to cause any immediate escalation of a wider military conflict, it is essential for the Red side to control the techniques being used so that such techniques will not lead to war with major actors on the Blue side. The measures should not cause any extreme widespread devastation, but preferably suitable levels of disturbance only.[12] In the literature, two possible forms of such disturbance are mentioned. The lighter form is called *distraction*, where decision-makers and populations fail to pay enough attention to the hybrid adversary's role and actions in the emerging crisis.[13] In this case, attribution of the actor behind CI disturbance would be vague in nature or even fail.

A more robust case mentioned in the literature would be *disruption*,[14] causing concrete losses and physical damages that cannot be repaired in the short term. The CI systems would have to adapt themselves to a new situation in which some parts of the earlier system would no longer be available, and the production level would be less than what it had been before the events (picture below).

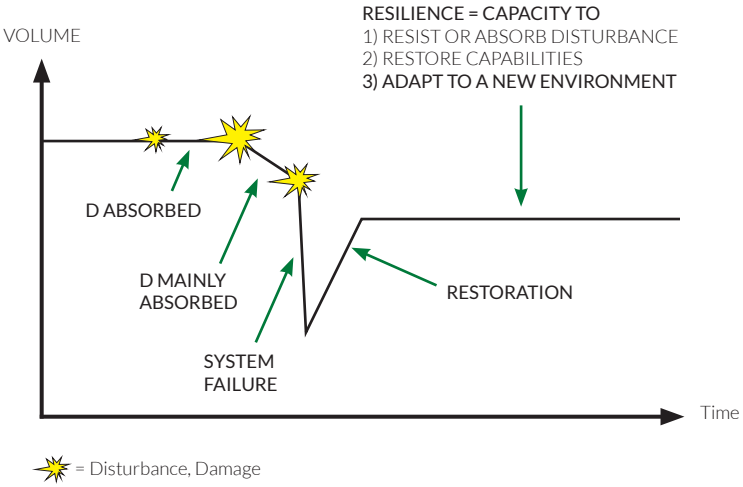
Between distraction (light damage only, no attribution) and disruption (serious damage), a space remains where CI disturbances factually reduce the affected side's capacity to act and to make decisions, but the CI systems are not entirely lost. They are left in a condition allowing them to resume operation in the near future, as explained in the examples provided in this paper.

In the "hybrid realm", any of the measures selected by an adversary should prevent the affected side from making the right decisions, but not lead to a direct, major military conflict. If one expects this kind of subtleness to be realistic, the hybrid toolbox available for hitting Critical Infrastructure would be useful in the hands of a competent adversary. The available asymmetric measures, together with the vulnerabilities of modern Critical Infrastructure, constitute a new threat when put together. This threat deserves to be named "Weapons of Mass Disturbance (WMDi)".[15]

12 The measures may be devastating from a local perspective (including individual companies, business sectors and even geographic regions) without being devastating enough to bring major actors to the brink of war.
13 In *Weapons of Mass-Distraction – Foreign State-Sponsored Disinformation in the Digital Age*, Nemr, Christina and Gangware describe the role of disinformation and misinformation in political campaigns that aim at distracting public opinions (pages 4–5). Measures resulting in the malfunctioning of Critical Infrastructure can possibly be used either to motivate or to strengthen such campaigns.
14 Michael A. Levi and Henry C. Kelly, "Weapons of Mass Disruption?", *Scientific American* (November 2002), pp. 77–79. Such devices as dirty bombs are often referred to as Weapons of Mass Disruption. They spread radioactive substance and can make vast land areas or significant amounts of property unexploitable until properly cleaned.
15 Naturally, the same tools and methods can be intentionally used for disruption and devastation during a prelude to a direct war.

PICTURE 8.
CI RESILIENCE AND DISRUPTION

Source: Igor Linkov



What are the appropriate countermeasures?

Apparently, one should work toward three purposes: 1) increase Critical Infrastructure resilience against hybrid threats (which would improve resilience against natural disturbances, too); 2) increase the probability of detecting breaches in systems and, should an operation take place, successful attribution of the actors behind it; and 3) facilitate the exchange of information and best practices within and across different fields of Critical Infrastructure.[16] Relevant technological requirements can be derived from these three aims. Some of the required improvements can be achieved through education, training and process development. The costs of such preparedness would be bearable. Some other requirements can best be achieved by improving technical standards and equipment. This leads to larger costs.

Critical Infrastructure is mainly run by private companies following a business logic and lean marginal profits. Their willingness to improve resilience against threats never seen before is very limited. When introducing the concept of hybrid threats to representatives from CI companies, one finds them interested in the topic. Some of them, though, point out that hybrid threats are primarily caused by external state actors and so preparedness is the responsibility of states, not that of private companies. This is partly true, but not a viable solution. No Western fiscal system can assume all of this responsibility now that the privatisation of CI has reached its current level. Companies must be made the main part of the solution, wherein authorities have a supporting and guiding role. Companies should consider how bad any hybrid influence or operation is for business, after all. Hybridity can also be used as an ingredient in hostile takeovers, which should make the owners interested.

States can do a great deal as well, and their main instrument is regulation. It must be borne in mind how open markets work, regardless of national borders. Whenever one state begins to impose costly regulations on some branch of business, this will have an impact on the competitiveness of busi-ness entities in the said country. Clearly, one should try to regulate them in a wider framework, such as the EU, or in the spirit of HybridCoE membership – within both the EU and NATO.

Another thing that states can and should do is to be prepared to financially assist some of the most vulnerable nodes in Critical Infrastructure. This can mean supporting stocks of critical material, technical systems or certain types of vulnerable market functions.[17]

A third emerging option for states is to develop EU- and NATO-level responses. In one recent Hybrid CoE workshop (February 2019), a medi-cal scenario was organised in which an epidemic spread rapidly throughout one of the participating states. National resources were not sufficient to deal with thousands of patients requiring intensive care.[18] It was discovered that, thanks to the assistance that would have been made available by Member States through NATO and by the EU through its Civil Protection Mechanism, thousands of lives could be saved.

16 Information Sharing and Analysis Centres (ISACs) is one solution developed first in the USA and now also in the EU. European Union Agency for Network and Information Security (ENISA): Information Sharing and Analysis Centres (ISACs), Brussels 2017
17 So far, the best example the author has come across is the Finnish National Emergency Supply Agency (NESA). Evidently, this is a best practice to share.
18 When talking of medical scenarios, it must be borne in mind that a naturally spreading disease may well have hybrid consequences (so we need/should not expect that so-called hybrid adversaries will use biological warfare against populations as a hybrid instrument). At any rate, if people start dying after any sort of a disaster that national actors are unable to cope with, the citizens of those nations will expect NATO and the EU to help. Failing that, those organisations will lose support.

Possibly, only one or a few Member States at a time would be targeted by a serious hybrid operation. Community-level (EU and/or Nato) assistance could then be regarded as an effective and efficient solution. Pooling saves money. The developing RescEU mechanism should be seen as a potential instrument to help Members States (or neighbours) cope with unlikely situations exceeding national capabilities.

References

Fiott, Daniel and Parkes, Roderick: Protecting Europe. The EU's response to hybrid threats. Brussels 2019 (ISS – European Union Institute for Security Studies)

Linkov, Igor; Trump, Benjamin: The Science and Practice of Resilience. Washington 2019 (Springer)
Nemr, Christina and Gangware, William: Weapons of Mass-Distraction - Foreign State-Sponsored Disinformation in the Digital Age. 2019 Park Advisors.

European Union Agency for Network and Information Security (ENISA): Information Sharing and Analysis Centres (ISAC's), Brussels 2017

Michael A. Levi and Henry C. Kelly: Weapons of Mass Disruption? Scientific American, November 2002, pp. 77–79.

Billing, Peter: Eskalation und Deeskalation internationaler Konflikte. Ein Konfliktmodell auf der Grundlage der empirischen Auswertung von 288 internationalen Konflikten seit 1945. Frankfurt 1992 (Lang Verlag)

NATO Press Release (2016) 118/8th July 2016 (For Nato's Seven Baseline Requirements)
Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. Brussels, 28.8.2013 SWD (2013) 318 final

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.


Hybrid CoE