The proliferation of cyber weapons -theory and mitigation-

Alexandru GEORGESCU
National Institute for Research and Development in Informatics – ICI Bucharest
alexandru.georgescu@ici.ro

Adrian Victor VEVERA
National Institute for Research and Development in Informatics - ICI Bucharest
victor.vevera@ici.ro

Carmen Elena CÎRNU
National Institute for Research and Development in Informatics – ICI Bucharest
carmen.cirnu@ici.ro

Abstract: Cyberspace has been designated by NATO as a new operational domain, but many countries, such as the US, preceded it. Cyber weaponry differs from kinetic weaponry and generate effects through non-kinetic means. Similar to the divide between nuclear weapons and conventional weapons, the availability and potential use of cyber weapons creates new dynamics, constraints and considerations in relations between states. Their usefulness in covert and overt warfare must be balanced with the insecurity they generate in the absence of rules and norms governing their use, which ultimately leads to collective insecurity. The article highlights key considerations on cyber weaponry and discusses the feasibility of non-proliferation efforts.
Keywords: cyber warfare, collective security, nonproliferation, resilience, cyber weaponry

INTRODUCTION

Cyber weapons and the proliferation of cyber weaponry have become current concerns for a world whose awareness is just now starting to catch up to the reality of the exposure it has to cyber threats. The critical infrastructures on which our lives are based, in transport, energy, finance, education, health, industry and others are, increasingly, controlled and coordinated through networked cybernetic systems which are integral to their functioning. Various categories of actors exploit this development for profit, ideology and tactical or strategic gain. Today, cyber-attacks are often a key element in the description of hybrid or asymmetric warfare, a type of conflict which renders geography irrelevant and brings a confrontation directly into the homes, offices and institutions of the citizenry.

This article acknowledges the protean or shifting nature of cyber threats, but aims to confine its view to that of the military stakeholders who are not just users of cyber infrastructure in their own right (modern military infrastructure, communication systems, smart munitions, cyber and electronic warfare etc.),

but, ultimately, may be considered a defender of last resort for all critical infrastructures inside a country or an alliance (Tatar et al, 2017). The tense International and regional situations have spawned a persistent low level confrontation in the cyber realm, often through proxy forces, which confounds both traditional strategic thinking as well as the governance mechanisms in place to regulate the legitimate use of force by a law abiding nation.

There is an element of uncertainty in the various taxonomies that have been developed for cyber threats. As we will see throughout this paper, cyber tools come in many different shapes and content, and their capacity to destroy is often a function of how they are used within a planned operation, rather than an inevitable result of their innate properties.

Therefore, a piece of malware embedded in computerized personal automobiles may be used to spy on the owners or to subsequently infect personal devices networking with the car, but may also be used in targeted assassinations or to create as much damage as possible in an intersection. Instances of cyber weapons like Stuxnet, which affected the feedback visualization mechanisms that allowed decision makers to adequately manage delicate equipment, are indicative of the levels of subtlety which are possible in this field, but also the dangers of loss of control, as Stuxnet ended up infecting computers throughout the world.

As for the proliferation of cyber weapons, this paper argues that it must be seen in a wider context of the development of the governance system of cyber confrontation, though proliferation itself is a very difficult proposition to handle, given the nature of cyber weapons.

CHARACTERISTICS OF CYBER WEAPONS

Cyber weapons are an interesting development, because, like any weapon, they either contain or inflict damage on the adversary. Unlike other weapons, they exist not in the physical realm, though their effects are felt there as well, but in cyberspace, an operational domain only recently recognized officially by NATO, whose characteristics are different from land, sea and air. It is decoupled from the geographical space and is rapidly shifting, requiring specific expertise to be read and mapped.

The US Department of Defense defines cyberspace as "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (DoD, 2013) and views it as having a physical network layer, a logical network layer and a cyber persona layer.

Osawa (2017) speaks of three types of cyber weapon use – sabotage, which paralyzes a network, most often temporarily, and reduces an adversary's capacity; subversion, which has a disruptive or destructive effect on the functions of a targeted system; and military-cyber-attack, where the cyber component is in play alongside a conventional military forces, wherein the cyber-attack is part of a unified stream of fire, potentially involving land, sea, air and cyber. Smeets (2018) finds that "offensive cyber operations refer to computer activities to disrupt, deny, degrade, and/or destroy" following a series of steps like reconnaissance, intrusion, privilege escalation, and payload dropping.

Cyber weapons also inflict damage selectively and reversibly to the adversary. This leads us to important properties regarding attribution, deterrence and response, where they differ from classic weapon systems.

Leuprecht et al (2019) point out that they are generally single use weapons, unless they have significant variations which imply that detection is not counter to concealment of another variant. Therefore, the use of cyber weapons will generally imply their reveal, which is not necessarily so important should the damage which was done be catastrophic. Cohen and Rotbart (2013) disagree and emphasize that the single use theory is unfounded and, rather, the widespread reuse of cyber warfare tools is the key of their evolution, through the reuse of modules and code.

Smeets (2018b) points out that cyber weapons can be prepositioned within an adversary's system for us at a later date, which will then expose it.

It may be detected beforehand, or the security gap which it is meant to exploit may be closed off through detection and resolution, or through routine software patching. While many weapons become obsolete, the cycle is especially quick with cyber weapons, even though Smeets (2018b) points out the cases of longer term usefulness of weapons like WannaCry and NotPetya on account of poor practices and security culture within targeted entities. At the same time, the limited duration of expected usefulness of a cyber weapon system may encourage its rapid use, with the possibility of escalation.

Intent is a difficult issue to discern by the entity under attack. The rapid growth in the number and pervasiveness of connections, especially as it related to the emerging Internet of Things, may enable cyber weapon systems to infiltrate unintended targets of high value, such as critical infrastructure operators and SCADA systems, or actual defense networks and weapon systems. This is due to the unrelated and shifting topology of the Internet, as well as opportunities to bridge divides between normally separate systems, through weapons that specifically try to enter air gapped systems or through high frequency communications.

Leuprecht et al (2019) emphasize that cyber weapons are not compatible with Westphalian logic of borders and attribution of aggression. Since the infrastructure is mainly privately owned and the geography of cyberspace makes path dependence much less likely, and much more fraught with danger, states are entering unknown waters by attempting to bring traditional military logic to the table and discuss a "cyber-Westphalian" system to ensure balance of cyber powers.

If we continue the comparison of cyber weapons to kinetic weapons, then we arrive at some key elements that define cyber weapons. For instance, they are used in cyber operations, cyber-attacks and cyberwarfare. At the same time, the use of cyber weapons in a military sense implies either or a mixture of counter value and counterforce use. The counter value use degrades the capacity of the adversary to support his war infrastructure, by targeting non-military entities such as the economic infrastructure, the political and administrative one, or the logistical one. The counterforce use degrades the warfighting capability of the adversary directly, by targeting military systems throughout the defense infrastructure.

The key element is uncertainty, which has always been associated with certain categories of weapons, such as nuclear ones, but never to this degree. And the uncertainty is doubled by the incipient stage of the rules and norms governing such engagements. This leads to variations in use which preclude the predictability of confrontation and makes it more likely that incidents will escalate uncontrollably. This is especially likely since cyber weapons seem to be a weapon of first resort, even though they are usable throughout every phase of a conflict, unlike nuclear weapons, which are employed, in theory, towards the end of a conflict, to force capitulation.

The risk of unintentional escalation is also inherent in the use of "hybrid warfare" and "measures short of war" in order to arrive as close to the tolerance level of an adversary without actually exceeding it. Cyber weapons are a prime instrument in the toolbox of states, especially given the issue not only of attribution to a particular state, but to any state at all, when it can just as well be an individual or a group acting on their own. However, the uncertainties of use and impact provides the possibility of unintended escalation or an attempt to "escalate to deescalate", where the targeted adversary replies in kind in order to establish a tit-for-tat dynamic which, in game theory, should lead to a reduction in attacks. There is also an asymmetry involved, in that democratic states have placed more controls on the use of cyber weapons than on the use of kinetic weapons, unlike non-democratic states and non-state actors. This is a possible result of a lagging understanding by political decision makers of the impact in the "real world" that cyber weapons may have, including as a form of collateral damage, as a result of the permeation of cyber and of connectivity into every facet of our lives.

The development of cyber weapons is also an aspect of proliferation, and this is an important decision for states. Hughes and Colarik (2016) argued that not every state should consider

entering such a competition, and that a careful analysis may reveal that it may even detract from security. They are among the authors who stress that cyber weaponry may be a sort of equalizer between small and large states, especially relative to the discrepancies in conventional and nuclear capabilities that may accrue, but this is not an absolute. Bigger states can and will invest more resources into development and protection, as well as allocate more personnel, while there is a limited scope for this distance to be covered by exceptional performance on the part of the smaller state (Hatch, 2018).

Their framework stresses analyzing the foundational elements of a state in question, the resource availability and policy alignment of cyber weapon systems, its cyber dependence, the benefits, feasibility and risks of the use of each cyber weapon and only then make a decision regarding an acquisition strategy.

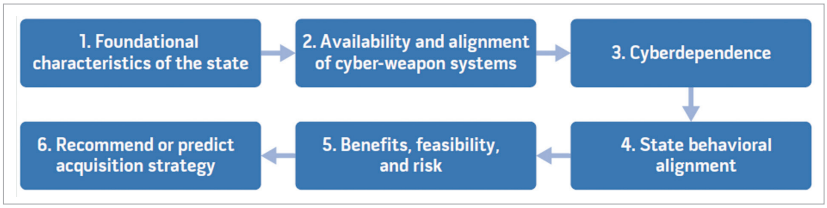

Fig. 1: *Cyber weapons acquisition framework (Hughes and Colarick, 2016)*

WIKILEAKS ON CYBER-PROLIFERATION

The new normal of constant information leaks by individuals with mercenary or ideological motivation has shined a light on the issue of cyber weaponry and its proliferations, at least as it pertains to American institutions. WikiLeaks (2017a) sums up the findings of some of the largest mass file leaks in history, as part of the "Year Zero" releases of the "Vault 7" leaks (8,761 files from the 2013-2016 period, according to WikiLeaks, 2017f).

Other entities have analyzed the files and compiled significant dossiers on cyber-related activity on the part of intelligence agencies.

According to WikiLeaks (2017a), the Center for Cyber Intelligence within the Directorate for Digital Innovation of the CIA had over 5.000 registered contributors in 2016 producing over 1.000 tools and systems for hacking, writing more lines of code than the entirety of Facebook. Other releases, such as WikiLeaks (2017b) and WikiLeaks (2017c), detail the activities and organization of this center and its subgroups on engineering, networks, targeted dissemination, software, infrastructure etc. The CIA capabilities also included cyber weapons supposedly retrieved from rival groups (WikiLeaks, 2017d), as well as catalogues of vulnerabilities in tech company products which they developed and maintained with partners intelligence agencies (such as 24 preexisting Android vulnerabilities) (WikiLeaks, 2017e).

A cursory listing of some of these revelations hints at the vast potential of cyber-weaponry proliferation. For instance, the Mobile Devices Branch focused on smartphones (WikiLeaks, 2017g), while the Embedded Devices Branch (WikiLeaks, 2017h) focuses, with applications such as "Weeping Angel" (WikiLeaks, 2017i), on smart TVs, and on modern cars and trucks(WikiLeaks, 2017j).

In order to infect computers of interest, running any one of multiple operating systems, the CIA developed and maintained inventories of zero day vulnerabilities (present at launch), air gap viruses for closed systems, jumping viruses like „Hammer Drill" (WikiLeaks, 2017k) for optical media, viruses for USB sticks (WikiLeaks, 2017l), systems that use images to conceal data (WikiLeaks, 2017m) or hidden areas of memory drives („Brutal Kangaroo", according to WikiLeaks, 2017n), as well as tools to ensure the persistence of malware infections (WikiLeaks, 2017o). Some of these actions contravened agreements regarding the reporting of zero day vulnerabilities to tech companies, so that they may be patched out before other entities discovered and used them as well (Healey, 2016), contributing to a general security malaise (WikiLeaks, 2017p).

While the ability to take advantage of nuclear proliferation is naturally limited by technology, infrastructure, finance and persistence in these attributes, in order to obtain enough fissile material for a nuclear weapon, assemble a functioning one and then miniaturize it for covert use or for delivery through ICBMs and

other missiles (which have to be developed as well), cyber weapons have a much lower threshold for development. They are also harder to retain. Once in the wild, it is doubtful that they can be contained, as they are easily copied and reproduced. This is why the WikiLeaks disclosure caused a stir, as they also contained indications, since reproduced in respectable media, that cyber weapons had been lost and subsequently made available in seconds to rival states, cyber criminals and teenage hackers. The very loss of information that engendered this discussion indicates the natural weakness of the current intelligence systems, especially in cyber, which have become reliant on outside contractors with little indoctrination and unknown ideological grounding.

Gaps also appear in any system trying to share information and tools, as well as coordinate, not just with allies, but also with dozens of peer agencies within the same community – such as the 16 agencies of the "intelligence industrial complex" of the United States. Cyber projects include:

• UMBRAGE (WikiLeaks, 2017q), which supposedly integrates malware from other entities and which can also be used to attribute cyber-attacks to other actors (WikiLeaks, 2017r);

• Fine Dining for customizing hacking attacks requested by case officers (And with categories like ‚Asset', ‚Liason Asset', ‚System Administrator', ‚Foreign Information Operations', ‚Foreign Intelligence Agencies' and ‚Foreign Government Entities');

• Improvise for configuration, payload setup and execution, vector selection and post-processing survey/exfiltration operations for all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor);

• HIVE, a multi-platform malware suite (WikiLeaks, 2017s) and associated control systems (WikiLeaks, 2017t), providing implantable programs for Windows, Linux, Solaris and MikroTik (Used in Internet routing) systems and a Listening Post (LP)/Command and Control (C2) infrastructure for communication with these implanted entities.

One of the unnamed sources was quoted by WikiLeaks (2017a) that they wanted to initiate a public debate on the "security, generation, utilization, proliferation and democratic control over cyber weapons". The quote reflects the assumption that cyber tools become weapons when they are used as such and that their flexibility in use makes even espionage tools potentially weaponizable.

GOVERNANCE OF CYBER WEAPONS

According to Gheorghe et al (2018) governance refers to the sum total of mechanisms, institutions, theories, rules, norms, laws or customs which provide the backdrop to government, which is the decision-making activity itself. The governance of cyber weapons use is an ongoing concern for the continuation of a rules-based liberal international order. Having played the role of "spoiler" in the existing framework, and allowing various state actors a new set of options to pursue their interests through coercion and subversion, cyber weapons are the focus of intense speculation on their future use.

While it may prove to be a hindrance, there have been those who have tried to assimilate cyber conflict into the wider framework on the Law of Armed Conflict and thereby adapt the existing system to its technological upheaval.

The discussions are mostly centered around the lawfulness of retaliation, but Gokce (2018) has analyzed the issue of active cyber defense (ACD) as a pre-emptive self-defense measure. Active defense is an affirmative, proactive and forcible action to detect and remove the threat of attacks, and appeared in cyber as a result of the unsatisfactory nature of passive cyber defense. In the latter approach, the surface of attack for an aggressor is maximized and he must only succeed once, whereas defenders need to succeed every time.

ACD does not necessarily contain offensive measures and can be confined to the networks which specifically require these protective measures, but other elements of ACD may create legal and ethical implications. ACD is "direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets" (Denning, 2013, via Gokce, 2018).

We can see in Fig. 2 that it is a middle position in

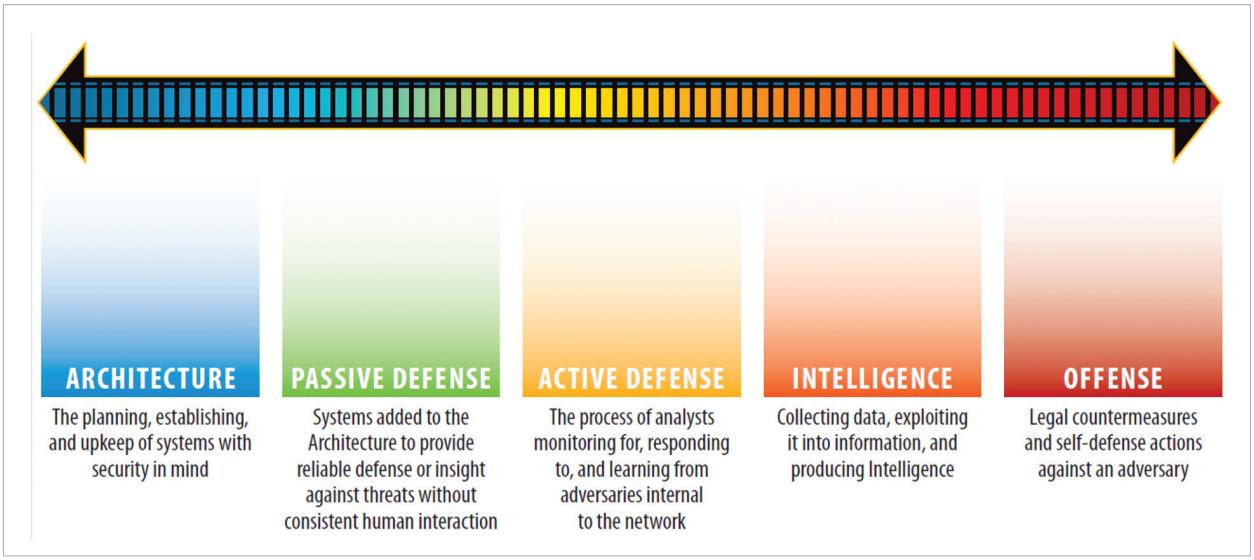

Fig. 2: *The sliding scale of cyber security (Lee, R., 2015)*

a road towards offensive measure. Dewar (2017) argued that there is a need for comprehensive cost-benefit analyses before the deployment of cyber defense techniques and that countries should choose resilience and build a toolbox from the following set for ASD: white worms, hack backs, address hopping and honeypots.

Article 51 of the UN Charter famously guarantees the right to self-defense. This would mean that measures even in the cyber realm require a state attack in order to be invoked. Sometimes, state can react to the imminence of an attack, and not wait for the actual armed attack to manifest. This is provided that the threat of attack is instant, overwhelming, leaving no choice of means or time for deliberation (Gokce, 2018). The state thus invokes anticipatory self-defense, which is customary in International Law. However, the state must also respect key conditions, in addition to imminence, such as proportionality and necessity. The former means that only the necessary force to counteract the attack shall be used and no more, thereby not exceeding the seriousness of the anticipated attack, nor, through its consequences, the anticipated harm. The latter presupposes that all other means of prevention have been exhausted or rendered irrelevant, and a forceful response remains the only viable option.

The International Court of Justice also created a "scale and effects" clause to determine whether an attack may be considered an "armed attack". Usually, this means that severe effects are expected from the materialization of the cyber threat, but retaliatory action may only come after the damages have been done. The simple act of infiltration is not sufficient, and anticipatory self-defense needs not only proof of infiltration, but also of destructive intention, such as would cause significant damage or loss of human life.

There is significant uncertainty in this framework of thought, both regarding the burden of proof being placed on the potential victim, and the actual meeting of the criteria for self-defense. The main problem is attribution, which was not considered a problematic issue in past confrontations. However, necessity and proportionality also suffer from problems related to the uncertainties of the use of cyber weapons. Also, the design of the ACD is also relevant, as it may, according toc circumstance or design, be oriented towards the use of force in self-defense or below the levels of the use of force (Gokce, 2018).

Leuprecht et al (2019) emphasize that the lack of governance in the field (with notable exceptions like the Budapest Convention on Cybercrime and the Tallinn Manuals) is producing collective insecurity, spawning a cyber security dilemma which forces states to develop a full panoply of cyberwarfare options (intrusion/detection, cyber-attack, cyber counter attack and cyber force) to "defend themselves and maintain the status quo".

In the absence of governance frameworks at global levels, solutions are likely to emerge among groups of like-minded states in NATO and the EU, while diplomacy in this anarchic cyber system will be used to at least clarify norms regarding use and force levels. The persistence of uncertainties regarding perpetrator, unintended consequences, target response, efficacy and the response from the international community also weighs heavily on decision making for law abiding states.

THE PROLIFERATION OF WEAPONS IN CYBERSPACE

Cohen and Rotbart (2013) argued that proliferation is the result of the use of cyber weapons and the subsequent reveal of their intended use and capabilities to the victim, who can then reuse them, even against the aggressor. The use of these means by states engaged in a veritable arms race with each other to cover avenues of attack and maintain their current level of security is understandable.

What is problematic is the proliferation of cyber weapons to non-state entities, who tend to be the point where uncontrollable proliferation starts. Whether they have achieved this one their own or with the help of a state sponsor, the procurement gap between state and non-state actors has been fast diminishing. Hughes and Colarik (2016) developed a model which could also be used to predict decision making regarding the proliferation of cyber weapons – "any ability to forecast cyber weapon acquisition on a state-by-state basis and thus monitor cyber weapon proliferation would be of substantial geopolitical benefit" since "geopolitical rivals may deploy cyber weapons as a means to advance national interests in this sphere of influence.".

Hatch (2018) explored whether declaring certain cyber weapon categories as weapons of mass destruction (WMD) would be useful for non-proliferation efforts, as it would mobilize significant resources within existing framework in order to prevent proliferation. He pointed out that there are only three criteria for designating a WMD – design as a weapon, mass casualties and international community classification as a special weapon – and cyber weapons already fulfilled two of them. The US Joint Chiefs of Staff had anticipated the possibility of classification being useful in 2004, and so they introduced the term WMD & E (Weapon of Mass Destruction & Effects) (Carus, 2012). The intent was to acknowledge not just the destructive potential of certain weapons, but also the disruptive potential of asymmetrical weapons available to terrorists and to rival states. Cyber weapons fit because the Joint Chiefs of Staff already acknowledge that they can cause "degradation, disruption, or destruction effects in the physical domain" (DoD, 2013). On the other hand, Caves and Carus (2014) had argued that it would be counterproductive for the US to declare cyber weapons as a WMD, since policy and strategic development were still in the nascent stage, and "they risked prematurely restraining a capability that could in reality maximize flexibility options for decision makers [...] a cyber WMD treaty would normally be associated with provisions to limit cyber's use, or set in motion steps to eliminate or control certain cyber threats" (Hatch, 2018).

Hatch (2018) echoes the 2018 US National Defense Strategy in supporting the idea that the US needs to be strategically predictable and operationally unpredictable in order to deter devastating cyber-attacks against it and its interest. To that end, Hatch (2018) proposes an "Attributed Response Assured" doctrine, which would emphasize attribution and the use of all elements of national power to respond after verification.

By designating certain cyber weapons as WMDs, the US may authorize military commanders to use cyber offensive means below that threshold on their own cognizance. His second proposal is to engage with the International community in defining those thresholds. Another option should this prove intractable is a "coalition of the willing" modelled on the 2003 Proliferation Security Initiative (PSI) that sought such a group "to use existing international and domestic laws to disrupt the transport of nuclear, biological, or chemical weapons and associated technologies to state and non-state actors suspected of

building a WMD program" (Hatch, 2018).

Deval (2016) explored the application of the Arms Control Treaty models to the cyber weapons issue and found them wanting in many respects, because of ambiguities, enforceability, verification and rapid technological change issues. They have important lessons to offer, however, though they require a shift in strategic culture away from achieving military balance and towards the reduction of the damages and suffering of conflict.

An interesting first application were the export controls on encryption technology introduced with the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods Technologies, which has an extensive list of adoptees. Litwak and King (2015) also gauged the limited and circumstantial use of this model, stressing that fundamental differences between domains means that "the bedrock of a state-based strategy to address cyber challenges is sound national policies, codified in domestic law and enforced" and thereby addressing the "cyber analogue to the passive sponsor challenge in counterterrorism". However, this still depends on getting states to limit their support of non-state entities, which is doubtful. Therefore, Litwak and King (2015) stress that, just as in the Cold War, "arms control needs to be buttressed by a robust strategy of deterrence in both its variants—deterrence by denial and deterrence by punishment".

Geers (2010) explored the idea of a Cyber Weapons Convention, similar to the Chemical Weapons Convention, the Biological Weapons Convention and the Ottawa Landmine Treaty (Ottawa Convention), stressing that they are made possible by three features which are absent in cyberspace, but potentially could be developed:

- The political will to control the use, because of the risks;
- The universality of the problem, given the lack of geographic barriers in cyberspace;
- A verification organization, one that also helps member states to improve cybersecurity.

The first two are already crystalizing, but the last one is challenging both politically, and operationally.

Morgus et al (2017) developed the "TrACE model" to integrate every possible configuration of cyber weapon non-proliferation strategy into a larger framework that describes its impact (fig. 3).

Morgus et al (2017) then listed five potential anti-proliferation measures, based either on international action – arms control agreements and export control agreements – or on tools for unilateral or coalition use – market manipulation to disrupt supply, enhance offensive and defensive capability and the diplomatic toolbox (fig. 4).

CONCLUSIONS

Cyber weapons are difficult to distinguish from the entire panoply of cyber tools for achieving state and non-state actor objectives.

In general, the weapons may feature a significant direct or collateral destructive capacity. States have scrambled to be able to adapt their strategic thinking to the realities of

	Transfers	Actors	Capabilities	Effects
Definition	The transfer of capabilities, knowledge, infrastructure, resources, or techniques between actors.	The entities responsible for developing and deploying malicious capabilities.	The software tools, techniques, or tradecraft used to produce some effect on a computer system.	The change produced on a computing system or attached hardware as a result of a capability's operation.
Categories	i) Intentional ii) Unintentional	i) Developers ii) Enablers iii) Defenders iv) Consumers	i) Knowledge ii) Tools iii) Platform iv) Infrastructure	i) Access ii) Espionage iii) Disruption iv) Destruction

Fig. 3: *TrACE Framework summary (Morgus et al, 2017)*

	TrACE Framework Element Addressed	Actor Effected	Current Feasibility	Longue Durée
Manipulate the market through purchasing power	Transfer and Capabilities	Developers, Deployers, and Enablers	Low	Yes
Enhance defensive capabilities	Capabilities and Effects	Defenders, Deployers	High	Yes
Enhance offensive capabilities (cyber and non-cyber)	Capabilities and Effects	Deployers	High	Yes
Diplomatic toolbox	Actors and Effects	Deployers	High	Yes

Fig. 4: *Anti-proliferation tools for unilateral use or within a coalition (Morgus et al, 2017)*

and ethics, of cyber-attacks. The results are not encouraging for those who would rather see cyber weapons restricted and controlled, not just with state conflict in mind, but also the pervasive risk of cybercrime and cyberterrorism.

The reality of our reliance on interdependent critical infrastructures leads to a collective insecurity which is steadily augmented by the spread of the Internet of Things and other developments which, while bringing new efficiencies and functionality, also multiply the attack vectors for dedicated cyber aggressors.

Under these conditions, states may be forced to engage in cyber warfare capability development simply to reduce the rate of deterioration of their security status and to, hopefully, provide deterrence from the well-resourced state actors who have the most significant capabilities in this regard.

ACKNOWLEDGMENT

This research was supported by Romanian Ministry of Research, project number 3N/2019.

REFERENCE LIST

*Carus, S.W. (2012), Defining "Weapons of Mass Destruction", Occasional Paper 8, Center for the Study of Weapons of Mass Destruction, National Defense University, https://www.researchgate.net/publication/281863975_Defining_weapons_of_mass_destruction

Caves, J., Carus, S.W. (2014) The Future of Weapons of Mass Destruction: Their Nature and Role in 2030, Occasional Paper 10, Center for the Study of Weapons of Mass Destruction, National Defense University, https://www.researchgate.net/publication/281863967_The_Future_of_Weapons_of_Mass_Destruction_Their_Nature_and_Role_in_2030

Christian Leuprecht, Joseph Szeman & David B. Skillicorn (2019), The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity, Contemporary Security Policy, Volume 40, 2019, Issue 3, ISSN 1743-8764, p. 382-407, https://doi.org/10.1080/13523260.2019.1590960

Cohen, D., Rotbart, A. (2013), The proliferation of weapons in cyberspace, in Gabi Siboni (ed.) (2013), Cyberspace and National Security, p. 105-127, Institute for National Security Studies, Tel Aviv, Israel, ISBN: 978-965-7425-51-0

Department of Defense (2013), Joint publication 3-12: Cyberspace operations, https://fas.org/irp/doddir/dod/jp3_12r.pdf

Dewar, R. (2017), Active Cyber Defense, ETH Zurich, November 2017, DOI: 10.13140/RG.2.2.19236.17287

Geers, K. (2010), Cyber Weapons Convention, Computer Law & Security Review, Volume 26, Issue 5, September 2010, Pages 547-551, https://doi.org/10.1016/j.clsr.2010.07.005

Gokce, Y. (2018), Active Cyber Defense as a Pre-emptive Defense Measure, in Tatar, U., Gokce, Y., Gheorghe, A., (2017), "Strategic Cyber Defense - a Multidisciplinary Perspective", IOS Press, NATO SPS Series D Vol. 48, ISBN 978-1-61499-770-2

Hatch, B. B. (2018), Defining a Class of Cyber Weapons as WMD: An Examination of the Merits, Journal of Strategic Studies, 11, no. 1 (2018): 43-61, https://doi.org/10.5038/1944-0472.11.1.1657

Healey, J. (2016), The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers, Journal of International Affairs, Columbia University's School of International and Public Affairs, Nov 01, 2016, https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process

Hughes, D., Colarik, A.M. (2016), Predicting the Proliferation of Cyber Weapons into Small States, Joint Force Quarterly, 2016, 4th Quarter 2016 (83), pp. 19 - 26 (8), http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/969646/predicting-the-proliferation-of-cyber-weapons-into-small-states/

Lee, R.M. (2015), The Sliding Scale of Cyber Security, SANS Institute online publication, https://www.sans.org/reading-room/whitepapers/ActiveDefense/paper/36240

Litwak, R., King, M. (2015) Arms Control in Cyberspace?, Wilson Center Policy Brief, https://www.wilsoncenter.org/publication/arms-control-cyberspace

Morgus, R., Smeets, M., Herr, T. (2017), Countering the proliferation of offensive cyber capabilities, in Global Commission on the Stability of Cyberspace (2018), Briefings from the Research Advisory Group, GCSC Issue Brief No. 1, p. 161 -187, New Delhi, November 2017, https://cisac.fsi.stanford.edu/publication/countering-proliferation-offensive-cyber-capabilities

Osawa, J. (2017), The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?, Asia Pacific Review 24(2):113-131, July 2017, DOI: 10.1080/13439006.2017.1406703

Smeets, M. (2018), The Strategic Promise of Offensive Cyber Operations, Strategic Studies Quarterly, August 2018, https://www.ctga.ox.ac.uk/article/strategic-promise-offensive-cyber-operations

Smeets, M. (2018b), Integrating offensive cyber capabilities: meaning, dilemmas, and assessment, Defence Studies 18(1):1-16, August 2018, DOI: 10.1080/14702436.2018.1508349

Tatar, U., Geers, K., Georgescu, A. (2017). "A Framework for a Military Cyber Defence Strategy Workshop– Final Report", in Tatar, U., Gokce, Y., Gheorghe, A., (2017), "Strategic Cyber Defense - a Multidisciplinary Perspective", IOS Press, NATO SPS Series D Vol. 48, ISBN 978-1-61499-770-2

WikiLeaks (2017a), https://wikileaks.org/ciav7p1/

WikiLeaks (2017b), https://wikileaks.org/ciav7p1/files/org-chart.png

WikiLeaks (2017c), https://wikileaks.org/ciav7p1/cms/space_15204355.html

WikiLeaks (2017d), https://wikileaks.org/ciav7p1/cms/page_2621753.html

WikiLeaks (2017e), https://wikileaks.org/ciav7p1/cms/page_11629096.html

WikiLeaks (2017f), https://wikileaks.org/ciav7p1/cms/index.html

WikiLeaks (2017g), https://wikileaks.org/ciav7p1/cms/space_3276804.html

WikiLeaks (2017h), https://wikileaks.org/ciav7p1/cms/space_753667.html

WikiLeaks (2017i), https://wikileaks.org/ciav7p1/cms/page_12353643.html

WikiLeaks (2017j), https://wikileaks.org/ciav7p1/cms/page_13763790.html

WikiLeaks (2017k), https://wikileaks.org/ciav7p1/cms/page_17072172.html

WikiLeaks (2017l), https://wikileaks.org/ciav7p1/cms/page_13762636.html

WikiLeaks (2017m), https://wikileaks.org/ciav7p1/cms/page_13763247.html

WikiLeaks (2017n), https://wikileaks.org/ciav7p1/cms/page_13763236.html

WikiLeaks (2017o), https://wikileaks.org/ciav7p1/cms/page_13763650.html

WikiLeaks (2017p), https://wikileaks.org/ciav7p1/cms/page_13205587.html

WikiLeaks (2017q), https://wikileaks.org/ciav7p1/cms/page_2621751.html

WikiLeaks (2017r), https://wikileaks.org/ciav7p1/cms/files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf

WikiLeaks (2017s), https://wikileaks.org/ciav7p1/cms/files/UsersGuide.pdf

WikiLeaks (2017t), https://wikileaks.org/ciav7p1/cms/files/DevelopersGuide.pdf