Cyberspace Escalation: Ladders or Lattices?

Martin C. Libicki
Maryellen and Richard L. Keyser Distinguished Visiting Professor
Center for Cyber Security Studies
United States Naval Academy

Olesya Tkacheva
Assistant Professor
Department of International Affairs
Vesalius College and Free University of Brussels (VUB)

Abstract: In any domain, deliberate escalation or de-escalation is an important tool in the management of crisis and conflict. Adroit use of such a tool to communicate intention and resolve presumes that all sides share an understanding that a move from one condition to another is or is not escalatory or de-escalatory. We argue that in cyberspace the distinction between the escalatory and de-escalatory use of cyber capabilities is less straightforward. It is more appropriate to conceptualise escalation as evolving like a lattice, allowing horizontal spill over to other domains as well as vertical movement that corresponds to greater intensity of conflict. We offer conceptual scenarios to illustrate this point and discuss the implications for NATO's doctrine for joint cyber operations and risk management.

Keywords: *NATO, cyber escalation, offensive cyber, cyber warfare*

1. Cyberspace Escalation: Ladders or Lattices?

In any domain, deliberate escalation or de-escalation is an important tool in the management of crisis and conflict. Adroit use of such a tool to communicate intention and resolve presumes that all sides share an understanding that a move from one condition to another is escalatory or de-escalatory. We contend, however, that cyberspace operations may challenge such understanding, looking like escalation in some respects but like the status quo or de-escalation in others. Such ambiguity should be appreciated by organisations such as NATO. Since the declaration of cyberspace as a military domain at its 2016 Warsaw Summit, NATO has upgraded its capabilities and updated its institutional and legal frameworks to operate in cyberspace as effectively as in other domains. This has entailed, among other measures, establishing a Cyberspace Operations Centre (CyOC) and integrating Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) into NATO operations. These allow the Allies to voluntarily contribute cyber capabilities to NATO missions to achieve desired effects while retaining command and control over them. Although NATO does not have its own offensive cyber capabilities, the growing importance of cyber operations for NATO's effective collective defence and deterrence requires a thorough understanding of how deploying cyber capabilities may affect conflict dynamics. It remains to be seen whether this will be perceived by conflicting parties as escalatory or de-escalatory.

The need to assess the implications of cyber for conflict dynamics is stated clearly in the *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*. This requires the consideration of interdependencies between cyber and other operational domains when evaluating the intended and unintended consequences of using cyber capabilities and also emphasizes the importance of risk management (NATO, 2020: p. 25). The doctrine, however, is devoid of any guidance on how to handle escalation in cyberspace. As noted in 2017 by Jamie Shea, the Deputy Assistant General for Emerging Threats:

> Whereas we have a good idea of how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyber attacks (Shea, 2017: p. 27).

This chapter illustrates why risk management in cyberspace could be more complicated than in other domains due to an inherited ambiguity about the escalatory or de-escalatory effects of cyber operations. We offer hypothetical scenarios to illustrate this point and then a model of escalation in cyberspace. Whereas previous studies have conceptualised escalation as changes in conflict intensity illustrated by the metaphor of an escalation 'ladder', our model characterises cyber escalation as a lattice. We show that escalation management strategies that assume escalation to be a ladder rather than a lattice may not work as expected. We develop a list of factors that should be taken into the account by NATO commanders when assessing and managing the risks of cyber operations.

A. Vertical Escalation in the Cyber Domain

The word escalation implies linear movement; up, maybe down, but never sideways. When applied to war or conflict, the metaphor is concise. A conflict at one level can move or be moved to the next higher—or, with de-escalation, lower—level. Given two levels of conflict, one is always and unambiguously higher than the other. Moving from one level to a higher level makes the level after that easier to reach, and therefore more likely. As a metaphor, escalation is literally one-dimensional. From this metaphor come concepts such as escalation dominance, escalate-to-de-escalate, and de-escalation signalling.

This linear conceptualisation has dominated scholarly debate on escalation in the cyber domain. Adversaries climb escalation ladders by first engaging in strategic signalling of cyber defence capabilities and then exploiting each other's networks, perhaps culminating in attacks on critical infrastructure (Kostyuk, Powell & Skach, 2018; Lin, 2012). From a commander's perspective, escalation requires understanding the thresholds that trigger an adversary's decision to escalate or de-escalate. The thresholds that trigger a response may be obvious only to the other side. As with conventional domains, in cyberspace, this opens doors to the miscalculation of the adversary's reaction and unintended escalation. The conflicting parties may not share an understanding of how cyber attacks fit into the other side's escalation ladder. Such a misunderstanding of the adversary's intentions could be more likely in cyberspace because of the greater prominence of emotions and cognitive biases that affect perceptions and the choice of corresponding countermeasures (Manzo, 2011; McDermott, 2019; Kreps & Schneider, 2019; Tomz & Weeks, 2020).

1) Escalation Lattice: Scenarios

We contend that if the effects of cyberspace operations are consequential enough, then the notion of escalation as a ladder may be misleading. Rather, escalation may be more like a lattice allowing horizontal as well as vertical movement. In truth, escalation was never strictly a ladder, despite Herman Kahn's focus on the escalation ladder metaphor in his classic study, *On Escalation* (1965). Besides the more commonly understood concept of vertical escalation—a change in intensity—there sits horizontal escalation in which the conflict moves into other theatres or domains (e.g., from sea to land), or includes additional participants. Horizontal escalation of the 1962 Missile Crisis, for instance, would have occurred if the Soviet Union had put its own 'quarantine' around Berlin, which it did not.

For the most part, though, in the bipolar world for which modern concepts of escalation developed, escalation meant vertical escalation. The literature on horizontal escalation is scarce and focuses only on the conventional domains (Epstein, 1983; Fitzsimmons, 2019). To the best of our knowledge, there have been no previous attempts to examine the relevance of horizontal escalation to cyberspace. Such conceptualisation is long overdue because in a conflict involving significant cyber operations it may not be obvious that one outcome is at a higher level than another.

To illustrate the possible ambiguities introduced by cyberspace operations—and this applies at both the tactical and strategic levels—consider a few hypothetical scenarios.

One, NATO and Russia confront one another in the Baltic over Russian attempts to expand its sea and air military exclusion zone around Kaliningrad. Each side is pouring naval and related air forces into the region: both are conducting operations in close proximity to one another. The situation is dangerous, not least because the next step appears to be a kinetic naval conflict. Russia (to pick one side) concludes that actual naval conflict would be a disaster but that it cannot give up the fight. So, while quietly withdrawing its naval forces from the stand-off, it launches devastating cyber attacks on the US homeland, aware that it could well suffer similar attacks from the US. Question: did it escalate or de-escalate?[1] The argument for a de-escalatory reading is based on the transition from potentially violent outcomes in the physical domains to costly but nonlethal outcomes in the virtual one. The case for an escalatory reading reflects the transition from regional, even off-shore conflict, to conflict against each side's homeland. Finally, whereas a naval confrontation or even combat can have a known endpoint because of the clear difference between war and peace, strategic cyber war may be harder to terminate because of attribution issues and the gauzy barrier between minor chronic and major acute cyber attacks.

Two, NATO is pushing back against the unprofessional and dangerous behaviour of Russian military jets in the Norwegian Sea. An incident occurs in which the ship of a NATO member nation has been damaged by an 'accidental' release of ordnance. In Brussels, leaders contemplate two options. One is to surge naval forces into the Norwegian Sea and alter the rules of engagement to raise the risk to Russian aircraft; the other is to initiate cyberspace and electronic warfare operations to suppress or at least confuse Russian surveillance capabilities during the confrontation. Which would be more escalatory? The first raises the risk of casualties. The second does not. But suppose Russian surveillance capabilities are suppressed and the Russians conclude it was due to cyberspace operations or Russia directly detects such cyberspace operations. If so, the Russians may well conclude that the purpose of such cyberspace operations is not limited to the confrontation at hand but is an attempt to blind Russian defences and lay the groundwork for a much broader set of NATO offensive kinetic operations. Worse; suppose further that these surveillance assets also serve as part of Russia's nuclear early-warning or command-and-control systems.

Three, after a tense standoff outside Narva (Estonia), Russian forces conspicuously withdraw several kilometres but at the same time, the volume of cyberspace intrusions into both civilian and military telecommunications that serve the border area appears to be rising. What is NATO to make of this? Is the crisis dissipating, as judged by the behaviour of Russian forces, or deepening due to the increased activity in cyberspace? If the Russians are using cyber attacks to create an opening for a raid-in-force, why are forces being demobilised? Could such behaviour—pulling forces back but ramping

[1] The question (albeit in a scenario involving China rather than Russia) was part of a final exam for Professor Libicki's students who had, a month earlier, participated in a war game with this scenario. Forty percent felt it was escalatory; sixty percent, de-escalatory. This split suggests the ambiguity is real.

up cyberspace operations—be like rolling dice and hoping for snake-eyes? Perhaps no single individual attempt to subvert NATO forces is likely to succeed and so continued mobilisation at the border is a waste of effort. But if one does succeed, it would be very useful to have forces nearby to exploit such an opening.

B. What, Exactly, Is Escalation?

There are many ways of assessing whether the transition from one state of conflict to another is escalatory. In a world in which escalation is one-dimensional, all the criteria would agree with one another: if A is more escalatory than B, it is more escalatory by every criterion that can be used to measure escalation. But, when escalation is multi-dimensional, A may be more escalatory than B by some measures and less by others, adding to the ambiguity.

Let us start with a basic definition of escalation as ‘an increase in the intensity or scope of conflict that crosses a threshold(s) considered significant by one or more of the participants’ (Morgan et al., 2008: p. 8). Metrics of intensity (vertical escalation) or scope (horizontal escalation) may or may not involve thresholds. The mutual escalation of both US and communist forces in South Vietnam *circa* 1965 was by degree—force levels rose on both sides. But they were not escalation by type: no consensus or even unilaterally declared threshold was crossed. Crossing a threshold implies a change in intensity, or at least opens the door to it. The atomic bombing of Hiroshima killed as many as the firebombing of Tokyo, but the former definitely crossed a threshold, albeit not one marked out in advance.

An additional helpful criterion that would apply whether or not escalation was a ladder or a lattice is whether the escalatory act is likely to be repeated or is, conversely, exemplary. The NotPetya cyber attack that caused roughly $10 billion of damage to the global economy in 2016-2017 but did not kill anyone clearly represented an increase in intensity, but nothing similar has taken place subsequently. If that trend continues, NotPetya, in retrospect, will have been less escalatory than a similar attack that would have been the first of many comparable cyber attacks. Russian DDoS attacks on Turkey in response to Turkey’s 2015 downing of a Russian jet ended once the point was made. In retrospect, therefore, its cyberspace response could not be deemed escalatory: it did not set a new standard for conflict in that dyad.

If escalation is a ladder, this implies that every step up makes reaching higher steps more likely. In many ways, this is why escalation matters: the greater costs involved in going from one level of conflict to another are self-evident, but the greater risk that accompanies such a move needs a theory of escalation to be seen. This rule need not pertain to every individual step. Herman Kahn’s treatment of escalation had 44 rungs, but he took care to state that no progression to all-out nuclear war would necessarily hit every step: skipping several at a time would be the rule. Nevertheless, the odds of reaching a nuclear Armageddon rose with each step up, as did the odds of reaching or surpassing any intermediate state. Granted, in some cases escalation could be an exemplary act by one side to force a de-escalatory effect if it scared the other side into seeking terms 'escalate-to-de-escalate' (Work and Winnefeld quoted in Schneider, 2017). But analysts argue that Russia's tactical nuclear strategy is not to seek terms through escalation but through a credible threat to escalate (Oliker & Baklitskiy, 2018) and it is possible that, while the use of tactical nuclear weapons may increase the odds of coming to terms, it may also raise the odds of further escalation to strategic nuclear exchange. Stalemates can be resolved in more than one way.

If escalation is a lattice, increases in intensity, at least as measured by one metric, may not necessarily raise the odds of further escalation, particularly if measured by a different metric. Take the first scenario, in which strategic cyber war—a systematic set of cyber attacks aimed at the other side's society and economy rather than its military—began as a substitute for a potential naval engagement. Now compare each choice in terms of its *further* escalation potential. The 2018 US *Nuclear Posture Review* (DoD, 2018) and a 2013 Defense Science Board report (ibid, 2013) held out the possibility that a sufficiently grave cyber attack on the critical infrastructure *could* lead to nuclear retaliation, although it is difficult to see that taking place without there being many deaths directly resulting from such an event. More plausibly, such a cyber attack could lead to a kinetic retaliation on the perpetrator's homeland,[2] which, itself, might escalate to nuclear weapons use. But a kinetic naval confrontation carries its own risks, especially if the losing side feels pressure to up the ante to the use of nuclear weapons as a way of taking out many naval targets at once. There are other pathways: one might lead from naval engagements to attacks on ports and their infrastructures. These might then be considered attacks on the homeland, giving rise to conventional attacks on other homeland targets that support military operations, and thence to nuclear attacks.

With multiple escalation pathways, it is not obvious that increases in intensity correlate with increases in the odds of further escalation. This applies especially if one set of paths comes from an intensification of force-on-force engagements, and another entails attacks on each side's homeland. This further complicates the assessment of whether one state of conflict is more escalatory than another.

C. Implications for Risk Management

A shift from ladders to lattices would complicate escalation management by multiplying ambiguities and uncertainties, but these are not always bad. It is as easy to imagine new possibilities leading to escalation foresworn or to de-escalation as it is imagining it leading to further escalation. This complicates

[2] During the May 2019 conflict between Israel and Hamas in Gaza, Israel declared that it had struck a building housing hackers who had just targeted Israel. Note, however, that kinetic war was already ongoing at the time of the cyber attack; also, it is not obvious that the building would have gone unstruck were it not for the cyber attack (Borghard & Schneider, 2019; Chesney, 2019).

risk management because of a greater risk of unintended escalation. Certain features of cyberspace operations may create more ambiguity over what is or is not escalatory due to several factors.

First, it is harder to understand the adversary's intentions in cyberspace. Cyberspace operations can potentially affect kinetic operations at all levels of conflict. As in the second scenario above, an intrusion meant to confound low-level kinetic confrontations can also confound more intense conventional kinetic operations or, in some cases, nuclear operations. The target may not know the attacker's intentions. Perhaps the attacker meant to have local effects (as in the second scenario), but the target reacted as if the attacker sought global ones.

Interpreting intentions becomes even more complicated in the light of multiple escalation pathways that may confound the tacit agreements associated with escalation management. If one side foregoes the opportunity to attack objects or use weapons that would escalate a conflict, it often does so under the assumption that the other side would do likewise. If the other side cheats, so to speak, it gains an advantage and makes the first look weak, which thereafter has less reason to restrain itself. Consider a situation in which neither side had previously escalated in a particular direction but then one side escalates in cyberspace. The other side could ignore it but would probably feel both pressured and entitled to react. It would ask itself whether the tacit agreement not to escalate in any domain was still in effect. If it determines that one direction—say, a cyberspace operation—is different from the traditional direction, it may well deem that the tacit agreement held in the kinetic arena and respond only in cyberspace. This tendency to treat cyberspace escalation as different in type from kinetic escalation would be reinforced if there were no tacit agreements in cyberspace that the cyberspace operation broke. This proposition is not absurd; many cyberspace operations are not only tactical but strategic surprises, in that the victim may not have believed that the attacker was interested in or allowed itself to carry out a particular operation. Conversely, the other side may deem any escalation in whatever medium a violation of the tacit accord and respond in whatever medium most favours it. One of the problems with a tacit agreement is its terms are never defined and hence each side may interpret what has been 'agreed' differently.

A further confounding variable merits note: is it the effort made, or the effect produced that marks escalation and indicates that a tacit agreement has been broken? This is relevant in cyberspace where most failing efforts fail quietly, while only those with effect are detected. Catching the other side trying to violate the agreement is evidence of bad intent and shows that the tacit agreement is no longer a constraint on the other side but, particularly in cyberspace, detecting an attempt in progress does not always indicate what the intention was and may not have left enough clues for positive attribution. In the physical world at least, the fact of failure makes a difference—the current US Administration has made a point of not responding to failed

North Korean missile launches (Fifield, 2017). In contrast, Israel responded with a cyber attack on one of Iran's ports in retaliation for unsuccessful cyber attacks on Israeli waterworks (Bergman & Halbfinger, 2020; Warrick & Nakashima, 2020).

Second, thresholds for escalation are more ambiguous in cyberspace. Compared to low-level violent conflict, cyberspace operations can be far costlier in time and therefore money. The bill for the many depredations of the 2017 NotPetya attack was roughly $10 billion. Yet, cyber attacks are rarely destructive and have not thus far killed anyone directly. To economists who routinely put a monetary cost on life in making cost-benefit calculations, many cyber attacks are more serious than military confrontations short of fully committed war. An ethicist who believes that the individual life is priceless such as Immanuel Kant would consequently draw a line between lethal and nonlethal operations that clearly put the use of lethal force above the line and cyber attacks, however costly, below it. This makes it more difficult to predict an adversary's thresholds for escalation. Will an attack on the electricity grid trigger the same reaction as an attack on financial institutions?

Despite the unending confrontations in cyberspace, strategic cyber war's potential to wreak serious damage on a modern economy is still a matter of dispute. The closest analogue may come from Russia's assaults on the Ukrainian economy. However, narratives about that conflict still focus on the loss of lives and territory brought by war and not the day-to-day difficulties associated with constantly losing online services because information systems have failed. The more consequential a strategic cyber war offensive, the more escalatory its introduction would be. The harder it is to guess its impact in advance, though, the greater the disagreement in assessing whether the start of such operations is escalatory.

The role of psychological effects is an additional factor that complicates the calculation of the desired effects. Even when cyber operations do not impose high economic costs, they might be perceived by state-actors as humiliating and trigger a disproportionate reaction to restore national dignity and regain trust in the eyes of the electorate. Emotions can trigger a response that by far outweighs the extent of economic costs.

Third, having multiple escalation paths obfuscates the de-escalation process. One possibility, alluded to above, arises from the fact that cyber war is understood differently by different parties. The media hypes the threat.[3] To war fighters, the disruption of cyber war is often just something else that could go wrong in an environment where things go wrong all the time. This disjunction allows a narrative in which one side's leaders trumpet their unsheathing of a bold new weapon as an indicator that they are still in the fight, but on the other side, cyber war adds complication but not necessarily catastrophe. Countries can thus mask their unwillingness to march to a confrontation by

[3] Consider the 3 July 2010 cover of the normally sober Economist which (unironically) uses a picture of a nuclear explosion as a metaphor for cyber war.

starting a new, albeit less lethal, one in cyberspace. But this option is not free. Because of delayed effects, potential rogue players and attribution issues, it may be more difficult to cleanly terminate a cyber war than to end its kinetic equivalent. It may trade an acute crisis for a chronic headache without a clear path to termination.

De-escalation would also look different if it were less like climbing down a ladder and more like working one's way down a lattice. But the difficulties may not echo those of escalation. Escalation and de-escalation are not opposite actions: the milestones on the road up rarely match those on the way down. In some cases, escalation may be publicised as a way of brandishing a capability or signalling a commitment: escalate to de-escalate. In other cases, escalation could be stealthy, to gain an advantage without sparking the other side to do likewise and thereby nullify the advantage. By contrast, de-escalation, withdrawal, is often a choice to temporarily yield an advantage to persuade the other side to impose constraints on itself; it must be effectively communicated if it is to do that. Given the tendency for parties in conflict to make worst-case assumptions about each other, one can expect that signs and portents of escalation would be eagerly seized upon as evidence of the other side's bad faith and intentions; inadvertent escalation is a serious concern in international relations (Posen, 1982). But the opposite is not so common. One side may eagerly await signs that the other is backing off[4] but, otherwise, may be suspicious of signals of de-escalation. A signal may be a mind game or a Trojan horse.

The ambiguities of cyberspace would hardly allay such suspicions; more likely they would exacerbate them. Consider one side that would signal de-escalation by ceasing cyber attacks. So, the other side stops seeing them. What would explain a fall-off in sightings? A confidence-building measure by the other side? A hiatus while other targets are being prepared? Evidence that its own defences are working better? If the other side counted all detected intrusions as potential cyber attacks, would a decrease in detections be considered a signal or evidence that the other side's cyberspace operations were now stealthier, or that its own ability to detect such operations has been compromised?

Any move to signal de-escalation by *substituting* cyberspace operations for kinetic operations confronts the possibility of more misinterpretation, as it assumes that both sides understand one to be less painful and less consequential than the other. But such understanding may be one-sided. Worse, events, such as a cyber attack on an infrastructure that yields indirect effects much costlier than their direct effects may turn the narrative around. If homeland cyber attacks are deemed more dangerous than some faraway kinetic conflict, something that one side thought signalled de-escalation would be read very differently.

[4] Consider the delusionary search for peace feelers for the Vietnam War in the later Johnson administration.

Fourth, the existence of multiple escalation pathways also complicates escalation dominance. Such a strategy requires one side to demonstrate that no escalated level of conflict would make the other side better off; a more muscular version is that one side will 'dominate' at every escalated level of conflict. But the greater the number of paths upward, the greater the burden on those seeking escalation dominance. They have to cover more bets. Conversely, demonstrating dominance only along costly escalation paths may, as above, create options for the other side to exploit escalation paths that call attention to themselves but are not particularly costly either as such or to the overall war effort. In other words, the existence of multiple pathways permits tolerable outcomes by channelling conflict in less damaging paths rather than having to suppress it entirely.

D. Implications for NATO's Operations in Cyberspace

At the Warsaw Summit, the Allies agreed to develop capabilities to operate in cyberspace 'as effectively as ... in the air, on land, and at sea' and to strengthen and to support the Alliance's overall deterrence and defence posture (NATO, 2016:§70). Our analysis calls into question whether the efficiency of cyber operations could be compared using the same metric used for kinetic options because of the inherent ambiguity with regards to its escalatory and de-escalatory effects. When escalation proceeds in a nonlinear manner, commanders should assess the effects beyond the threshold at which cyber capabilities are used. Even though both cyber and kinetic options could generate similar immediate tactical effects, for example by piercing an Anti-Access/Area Denial (A2/AD) bubble, the strategic implications of using cyber capabilities are more ambiguous and harder to predict. By widening the conflict to multiple domains, NATO could obscure its hand regarding the next move and exploit this ambiguity to gain tactical and operational advantage. Conversely, it also implies that NATO commanders could also misread the intentions of an adversary in the cyber domain. The conceptual shift from ladders to lattices that comes from considering the role of efficacious cyberspace operations in a crisis or conflict would, not surprisingly, complicate escalation management. Likewise, it introduces ambiguities and uncertainties.

This also implies that risk management in cyberspace requires developing in-house expertise not only of adversary's technological vulnerabilities, but also of threat perceptions, corresponding thresholds and political constraints that can influence subsequent responses. It entails greater Human Intelligence and open-source intelligence sharing among Allies whenever cyberspace effects are being sought. This also requires more refined scenario development for NATO exercises. Its goals would be to assess the technological capabilities available to achieve the cyberspace effects and understand how the use of such capabilities may appear to relevant actors.

2. CONCLUSIONS

It is difficult enough to determine the degree of escalation in a confrontation involving only cyberspace operations. Once other elements of power are also involved, comparisons between the real and the virtual can yield different conclusions from different perspectives. The challenges to NATO are not entirely virtual; as there are real-world elements ranging from unidentified combatants (sometimes known as little green men), proxy warriors and unprofessional military activities to the brandishing of nuclear weapons. So, comparisons—is *this* worse than *that*—are inevitable.

The difficulty of determining whether shifts in a confrontation towards cyberspace are or are not escalatory is of a piece with the many ambiguities of this newest domain of conflict. If NATO aims to 'win' any possible confrontation with its opponents, regardless of where it leads, labelling any one development as being escalatory is secondary. But if NATO wants to manage these confrontations and settle them at modest cost and risk to the Alliance's values, then correct understandings of escalation begin to matter.

NATO faces several paths. One is to de-emphasise signalling altogether and accept that modern confrontations will be too ambiguous and noisy for one side's implications (or even statements) to translate with fidelity into the other side's inferences. Russia will reach its own conclusions about NATO regardless of what NATO tries to convey, especially when through wordless deeds. The other is to use dialogue to help build a foundation for evaluating and responding to the evolution of confrontations. A great deal of the ambiguity in evaluating cyberspace operations is inherent in the medium itself, so dialogue may not guarantee that all such shifts and signals garner the correct response. Yet, it may narrow the range of plausible responses and reduce the occurrence of nonlinear reactions that lend unnecessary instability to such confrontations.

3. REFERENCES

Bergman, R. & Halbfinger, D. M. (2020) Israel hack of Iran port is latest salvo in exchange of cyberattacks. *The New York Times*. 20th May. Available from: https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html [Accessed 12th July 2020].

Borghard, E. D. & Schneider, J. (2019) Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal. *The Washington Post*. 9th May. Available from: https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/ [Accessed 21st September 2020].

Chesney, R. (2019) Crossing a cyber Rubicon? Overreactions to the IDF's strike on the Hamas cyber facility. *Lawfareblog.com*. 6th May. Available from: https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility [Accessed 21st September 2020].

Epstein, J. M. (1983) Horizontal escalation: sour notes of a recurrent theme. *International Security*. 8 (3), 19-31. Available from: http://www.jstor.com/stable/2538698 [Accessed 10th July 2020].

Fifield, A. (2017) U.S. says it ignored North Korea's latest missile launch because it failed; VP Pence arrives in Seoul. *National Post.* 16th April. Available from: http://news.nationalpost.com/news/world/u-s-ignores-north-koreas-latest-missile-launch-because-it-failed-as-vice-president-heads-to-asia [Accessed 2nd June 2020].

Fitzsimmons, M. (2019) Horizontal escalation: an asymmetric approach to Russian aggression? *Strategic Studies Quarterly*. 13 (1), 95-113. Available from: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-1/Fitzsimmons.pdf [Accessed 7th July 2020].

Kahn, H. (1965) *On Escalation: Scenarios and Metaphors.* New York, NY, Praeger.

Kostyuk, N., Powell, S. & Skach, M. (2018) Determinants of the cyber escalation ladder. *The Cyber Defense Review*. 3 (1), 123-134. Available from: https://www.jstor.org/stable/26427380 [Accessed 20th June 2020].

Kreps, S. & Schneider, J. (2019) Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*. 5 (1), 1-11.Available from: https://doi.org/10.1093/cybsec/tyz007.

Lin, H. (2012) Escalation dynamics and conflict termination in cyberspace. *Strategic Studies Quarterly*. 6 (3), 46-70. Available from: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-3/Lin.pdf [Accessed 8th August 2020].

Manzo, V. (2011) Deterrence and escalation in cross-domain operations: where do space and cyberspace fit? *Strategic Forum*. 272, 1-8. Available from: https://www.questia.com/library/journal/1G1-291503426/deterrence-and-escalation-in-cross-domain-operations [Accessed 13th July 2020].

McDermott, R. (2019) Some emotional considerations in cyber conflict. *Journal of Cyber Policy*. 4 (3), 309-325.

Morgan, F.E., Mueller, K.P., Medeiros, E.S., Pollpeter, K.L. & Cliff, R. (2008) *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA, Rand Corporation.

NATO (2016) Warsaw Summit Communiqué. 9th July. Available from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 24th October 2020].

NATO (2020) *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed 21st July 2020].

Oliker, O. & Baklitskiy, A. (2018) The nuclear posture review and Russian 'de-escalation:' a dangerous solution to a non-existent problem. *War on the Rocks*. 20th February. Available from: https://warontherocks.com/2018/02/nuclear-posture-review-russian-de-escalation-dangerous-solutionnonexistent-problem/ [Accessed 8th August 2020].

Posen, B.R. (1982) Inadvertent nuclear war? escalation and NATO's northern flank. *International Security*. 7 (2), 28–54.

Schneider, M. B. (2017) Escalate to de-escalate. *Naval Institute Proceedings*. 143/2/1368. February. Available from: https://www.usni.org/magazines/proceedings/2017/february/escalate-de-escalate [Accessed 21st September, 2020].

Shea, J. (2017) How is NATO meeting the challenge in cyberspace. *Prism*. 7 (2), 18-29. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/1044679.pdf [Accessed 14th July 2020].

Smeets, M. (2019). NATO member's organizational path towards conducting offensive cyber operations: a framework for analysis. In : Minárik, T., Alatalu, S., Biondi, S., Signoretti, M., Tolga, I., and Visky, G. (eds.) *2019 11th International Conference on Cyber Conflict: Silent Battle*, 28-31 May 2019, Tallinn, Estonia. NATO CCDCOE Publications. pp. 1-15. Available from: doi:10.23919/CYCON.2019.8756634.

Tomz M. & Weeks, J. LP. (2020) Public opinion and foreign electoral intervention. To be published in *American Political Science Review*. [Preprint] Available from: https://iriss.stanford.edu/sites/g/files/sbiybj6196/f/publications/public_opinion_and_foreign_electoral_intervention.pdf [Accessed 1st June 2020].

U.S. Department of Defense (2013) Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. January. Available from: https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf [Accessed 21st September 2020].

U.S. Department of Defense (2018) Nuclear Posture Review. February. Available from: https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx [Accessed 21st September 2020].

Warrick, J. & Nakashima, E. (2020) Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*. 18th May. Available from: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html [Accessed 18th May 2020].