The role of cyber operations in Iran's policy toward the United States: A qualitative perspective

August 2021

2486499M

19108656

23098904

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 24056

Supervisor: Tomáš Kučera

Date of Submission: August 1, 2021

Abstract

This study examines the role and utility of low-severity cyber operations in one state's policy toward another within the context of a long-term hostile feud. This study has fulfilled this task through an explanatory qualitative analysis with cyber operations as an embedded unit of study. The subject of research is the policy of the Islamic Republic of Iran toward the United States in the time spanning from the historic agreement of the Joint Comprehensive Plan of Action (JCPOA), also known as the Nuclear Deal, in July 2015 through 2020. The *role* of the cyber operations in Iran's policy is examined by juxtaposing the pattern of escalations and de-escalations occurring in the context, and in the political and military domains conducted by the Islamic Republic with their deployment of cyber operations. Through this pattern matching, this study identified a visible relative restraint in the cyber domain during the first years following the conclusion of the JCPOA, as the Islamic Republic had obtained its top strategic goal, defined as eliminating all sanctions burdening its economy. Iran's cyber operations towards the United States re-emerged when Washington exited the Nuclear Deal in 2018 and began re-instating sanctions, and the operations were intensified when Tehran began steadily escalating in the political domain the following year. The *utility* of the operations was determined by examining the pattern detailed and the direct and indirect implications of the operations seemingly benefiting the Islamic Republic.

The identified pattern suggests that the operations fulfill the function of signaling broad policy stances and are generally not used as a precision tool. The cyber operations appear to be deployed as a supplementary measure of signaling tied to the moves in the political domain. Meanwhile, the military moves are dual in aim and appear to follow a parallel rationale. Although the *direct* effects of the Iranian cyber operations were almost absent, the indirect and communicative effects were positive for Tehran. The psychological aspect of cyber operations prove a central part of their effectiveness for the Islamic Republic, making resistance visible, yet with vanishingly little escalation risk. The findings of this study strengthen the scholarship on policy in cyberspace that holds that cyber operations of low-severity *can* have a positive effect on a state's stance in an adversarial relationship. This research indicates that the entrance of cyber operations in a dynamic feud does not have to increase the escalation risk in the relationship because the wielder of the operations can obtain a needed effect through low-severity operations. Thus, the presence of cyber operations can be seen as stabilizing because they provide an option for signaling discontent with low escalatory risk. The study further provides evidence on how low severity cyber operations can function as conscious signaling tools despite their covert nature, supporting their status as 'open secrets' alluded to in segments of relevant literature.

Keywords

Cyber Operations, Cyber Policy, Escalation, Coercion, Non-Coercive Cyber Operations, The Islamic Republic of Iran, The United States of America, The JCPOA, Iran Nuclear Deal, Trump Administration, Maximum Pressure Campaign, Cyber Competition, Cover Cyber Operations, Political Escalation, Military Escalation, Cyber Escalation.

Acknowledgements

I would like to extend my thanks to my supervisor, Dr. Tomáš Kučera at Charles University, for insightful guidance through a challenging project undertaken in trying times.

Many thanks to Torbjørn Kveberg, Michael Mayer and Mats Rjaanes at the Norwegian Defence Research Establishment for insightful discussions, support and guidance in all matters cyber, methodology and policy.

My gratitude to my dear family, friends and dearest Herman, for invaluable encouragement and support.

List of appendices

List of abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
IAEA	International Atomic Energy Agency
IRGC	Islamic Revolutionary Guard Corps
IRNA	Islamic Republic News Agency
ISA	Iran Sanctions Act
JCPOA	Joint Comprehensive Plan of Action
UNSC	United Nations Security Council
UNSG	United Nations Secretary-General
USDoD	United States Department of Defense
USDJ	United States Department of Justice
USDS	United States Department of State
USDT	United States Department of the Treasury

Table of contents

Chapter 1 - Introduction

Visitors of several news websites with ties to the Islamic Republic of Iran woke up to a surprise in late June 2021. Upon entering the sites of Press TV, Al-Alam and others, they were met with the seals of the United States' Federal Bureau of Investigation (FBI) and Bureau of Industry and Security. The websites showed a notice stating that the domains had been seized in a law enforcement operation. The United States Department of Justice (USDJ) cited the spreading of disinformation and breach of sanctions rules as reasons for the takedowns (USDJ, 2021). The US sanctions regime details that entities with ties to the Islamic Revolutionary Guard Corps (IRGC) are prohibited from obtaining services in the United States without special licensing, services such as domain hosting on US infrastructure (Talmazan and Arouzi, 2021; United States Department of Justice, 2021). An official Iranian news outlet deemed the takedowns illegal and a "terroristic policy" against the independent media (IRNA, 2021).

The digital domain has become an important arena for state interaction, power politics and competition. The June takedowns are an example of the utility of cyberspace for advancing policy in the context of the longstanding standoff between the US and Iran. Much ink has already been spilled on developing an understanding of how the differences between conventional policy arenas and cyberspace are playing into the opportunities and vulnerabilities of states. This study aims at contributing to a segment of this debate through presenting an alternative approach for understanding the usefulness of cyber operations in a dynamic interaction over time.

There is a disconnect between the type of activity emphasized by the academic literature on strategy in cyberspace and the activity that constitutes the largest component in the domain. The focus in the literature has been on the highest echelons of conflict. Scholars have pointed out the oddity that the language of military strategy has gained such deep roots in this field when most of the activity that occurs in cyberspace has little to do with the use of force (Rovner, 2019).

This position is backed by large empirical studies that have revealed how the vast majority of state activity in cyberspace cannot be explained by the logic of coercive strategies. Nevertheless, the scholarship attempting to explain this activity remains preoccupied with this segment of international relations theory. This author holds that there is a need for further research advancing a better understanding of the utility of policy through cyberspace that is non-coercive and occurring in a strategic space short of war.

Another tendency in the literature on this topic is to examine cyber operations in isolation from other tools of statecraft. This classical approach fails to absorb a key issue for understanding the utility and importance of a segment of policy, namely its role vis-à-vis a state's remaining policy tools. Cyber operations are one group of tools a state may employ to advance its interests and one that can fulfill a plethora of functions. This author would hold that this approach is missing in the study of policy in cyberspace. In order to advance the understanding of the nature of cyber operations as policy tools in the strategic space short of war, they should be examined from the point of view of what role they have in relation to conventional tools of statecraft and under which circumstances they are deployed.

1.2 The research question

The aim of this study is to contribute to a better understanding of the role and utility of non-coercive cyber operations in the strategic space short of war. This is important because it will direct much needed attention to the segment of state activity in cyberspace that constitutes the largest part of the total activity in the domain. A key assumption of this study is that the wielder of cyber operations is likely to use them in a way that helps to advance their interests, but in a non-coercive manner and avoiding escalations of significance. This author holds that understanding this utility should be done by examining the role of cyber operations vis-à-vis the state's use of conventional policy tools in relation to the development in the context. What can the timing, target choices and pattern of behavior vis-à-vis conventional tools of statecraft reveal about the role and utility of this type of cyber operations? This author holds that establishing a pattern of behavior that reveals when a state *chooses* to use cyber operations within a dynamic relationship should advance an understanding of the role of cyber operations in this state's policy.

The research question guiding this study is "what is the role of cyber operations in Iran's policy toward the United States?" This will be answered through a qualitative analysis of the case study of the feud between the Islamic Republic of Iran and the United States. The analysis will examine Iran's use of cyber operations as an embedded unit of study and view its utility in relation to the Islamic Republic's usage of conventional policy tools and the development in the context. Iran has been chosen as a unit of study because it is an eager user of cyber operations to advance its interests. Iran has steadily invested in its cyber capabilities in the last decade and is now commonly placed fourth or fifth in offensive capability worldwide, with the United States leading (O'Flaherty, 2020). This study is choosing an unambiguously *uneven* dyad in terms of power because the weaker party is more likely to remain in the strategic space short of war. Additionally, cyber operations have come to be understood as a tool favored by weaker states as an asymmetric tool. Therefore, it should be expected that the weaker party make the fullest use of this class of policy tools.

Two levels of analysis will be conducted to answer the research question guiding this study. The first level examines the pattern of behavior of Iranian cyber operations seen in relation to the development in the context and Iranian use of conventional policy tools between July 2015 through 2020. The conventional policy tools will be understood as a divide between *political* and *military* moves, along a horizontal-vertical escalation model. This first level of analysis will test the hypothesis "the cyber operations will follow the escalation dynamic in the other domains."

The second level of analysis will take a step back and examine *how* the cyber operations are useful for Iran. This should include both the direct and indirect effects of the operations in question, as well as the pattern identified in the first level of analysis. According to the theoretical framework guiding this study, states may engage in the steps associated with the moves of escalation in order to gain an advantage in the strategic space of non-coercive strategies (Kahn, 2017, p. 7). This entails that an actor may make moves that correspond to vertical or horizontal escalation that are of low severity and do not escalate the overall temperature in the feud, but are aimed at increasing the actor's power or chipping away at the opponent's sources of national power (Fischerkeller and Harknett, 2019a, pp. 274–5).

The empirical analysis of this study concludes that the pattern of behavior of Iranian cyber operations reveal a strategy of conscious signaling. The hypothesis is confirmed in light of the escalation dynamic at a broad level, but only in a few instances do the operations appear to be direct responses to developments in the relationship. This indicates that the operations fulfill the function of tools signaling broad policy stances and are overall not used as a precision tool. Part of the utility of the operations for the Islamic republic lies in exposing vulnerabilities in the Unites States and make visible their own resistance to advancements of US policy without risking escalating the hostilities in the relationship significantly.

The following chapter will outline relevant literature on the topic and situate the contribution of this study within the academic field. The review of the literature will further suggest expectations of what may be found through the empirical analysis. Chapter 3 will fulfill the research design and methodology component of this study and map out the strategy for data collection and analysis, before pointing to some limitations of the research. The empirical analysis conducted in chapter 4 will be fulfilled through qualitatively analyzing the pattern of behavior in the timeframe chosen, before critically interpreting and analyzing the pattern and its meaning. Chapter 5 will discuss the findings of the empirical analysis in relation to the academic field and conclude by presenting criticisms of the analysis and suggestions for future research.

Chapter 2 – Review of the literature

2.1 Introduction

Over the last decade, scholars examining the potential for destruction through cyber operations have nuanced the earliest alarmist views on the matter. [1] This has contributed to a better understanding of the actual room to maneuver that states and other cyber actors enjoy in the cyber domain. However, there are still gaps in the literature regarding how to understand how cyber operations function as tools for policy in a *non*-coercive manner. Coercive strategies remain central in the literature on states' activities in cyberspace, but non-coercive *interaction* is more in line with the empirical record. Non-coercive cyber operations tend to be classified as espionage and then ignored for further examination. The dynamics, aims and indirect effects of this class of cyber operations are not well understood, and have been sparsely treated in the literature. This chapter will outline relevant debates on how cyber operations are understood as a tool for policy and strategy. It will begin by mapping out approaches to cyber operations and escalation. It will then discuss research on the empirical record of cyber activity before debating approaches to understanding the non-coercive interaction in cyberspace, including what gains are achievable and of strategic significance short of war. The final section will expand on understandings on the role of cyber operations in a state's arsenal of policy tools.

2.2 Cyberspace and escalation

Escalation theory has been a central pillar of the debate on the impact of cyberspace on international relations. Deliberate escalation is an important tool for states to communicate resolve, intentions, capabilities, and red lines (Libicki and Tkacheva, 2020, p. 60). How it is understood has varied somewhat. The seminal work *On Escalation: Metaphors and Scenarios* of Herman Kahn (2017,

---

[1] For a comprehensive overview of the early literature on cyberwar, see (Healey and Grindal, 2013). Denning (2009) and Cavelty (2008) discuss the debate on threat inflation of the topic. McConnell (2009) is a good example of an alarmist approach to the impact of cyberspace on international relations.

p. 3) describes escalation as “an increase in the level of conflict in international crisis situations.” Thresholds are central to Kahn’s escalation concept, and he established a ladder of 44 rungs of escalation signifying gradual increase in severity.[2] Libicki and Tkacheva (2020, p. 64) hold that escalation does not have to involve thresholds, but an alteration of the efforts, either in *degree* or *type*. Morgan et al. (2008, p. 8) view an escalation having taken place when “at least one of the parties involved believes there has been a significant qualitative change in the conflict as a result of the new development.” Others have developed Kahn’s escalation theory further by altering slightly the ‘ways’ a state may escalate (Morgan *et al.*, 2008; Libicki, 2012; Cavaiola, Gompert and Libicki, 2015). The classical core remains a *vertical* - *horizontal* escalation model where the former signifies increasing intensity within one domain and the latter entails beginning activity in a new domain.

Voluntary escalation is covered by one segment of the literature, but it is the conditions for and implications of accidental and inadvertent escalation that have been most idly examined by scholars. Seminal works have evidenced how escalation may happen as a result of bureaucratic bargaining processes or standardized programs for policy (Allison and Zelikow, 1999), misrepresenting risk (Schelling, 1967, chap. 3), or through the security dilemma (Jervis, 1978). The reason for escalation theory being so commonly used as a theoretical lens for studying state interaction in cyberspace that “[t]here is a widespread view among practitioners and scholars that cyberspace is defined by an inherent potential for dangerous escalation dynamics between rivals.” (Borghard and Lonergan, 2019, p. 122). According to this view, what might begin as a low-severity operation within a strategic space *short* of war could trigger a spiraling escalation leading the actors to cross a threshold into the strategic space of armed confrontation. Cyberspace has from early on been viewed as being *offense dominant* because of relative anonymity, challenges for swift attribution and the lack of established thresholds (Lynn, 2010; Libicki, 2012; Lin, 2012a; Cavaiola, Gompert and

[2] See Kostyuk et al (2018) for a take on defining an escalation ladder of cyber operations.

Libicki, 2015; Rid and Buchanan, 2015; Healey, 2019). The offense-defense theory states that the balance[3] between the offensive and the defensive stances will determine the efficacies of security strategies. When the offense has the advantage, either from relative costs or technological attributes, an offensive strategy is the most advantageous, triggering a spiraling armament dynamic which increases the probability for war (Lynn-Jones, 1995, p. 661). According to this view, the technical attributes of cyberspace incentivizes behavior that risks inadvertent escalation. The qualities of the 'ways' states can cause effect through cyberspace also plays into the implications of the domain. The transitory nature of cyber 'weapons[4]' has been expanded on in recent scholarship, underscoring the fact that cyber capabilities are temporary in nature, have uncertain effects and can be reversed (Smeets, 2018a; Borghard and Lonergan, 2019). What kind of behavior this transitory nature incentivizes is a topic for debate. Libicki (2007, p. 87) argues that it makes actors practice restraint and save their capability for the right moment. Krepinevich (2012) disagrees with this view and makes the case that the limited window of opportunity for effect might encourage an actor to use the capability sooner rather than later. The implications of this debate rely on the *level of severity* of the effects of the capabilities in question. However, if cyberspace is indeed inherently escalatory, this begs the question of why we have not yet seen large escalations from this domain.

Gartzke and Lindsay (2015) answered this question by disputing the root assumptions about the offense-dominance in cyberspace. They argued that the qualities of cyberspace giving advantage to offensive postures only apply to 'nuisance attacks' of low severity (2015, pp. 324–5). Destructive attacks of significant severity require funds, time and skill of a completely different scale

[3] "The offense-defense balance is the amount of resources that a state must invest in offense to offset an adversary's investment in defense." (Lynn-Jones, 1995, p. 665)

[4] There is a division in the scholarship regarding whether to use the term 'cyber weapons' or 'cyber capabilities'. Lucas Kello (2017) is a well-known proponent for the 'weapons' term. Van Puyvelde and Brantly (2019, p. 74) argue that 'capabilities' are most fitting because "one cyber capability does not necessarily equate to another in the same way that one bullet is similar to other bullets."

(Watling, 2020). They further hold that the qualities traditionally attributed to the dominance of offense are to a larger degree giving advantage to *deception,* defined as a covert "strategy designed to improve one's prospects in competition" (2015, p. 327). They argue that the internet's capacity for deception has laid the groundwork for the potential for all malicious activity conducted through the domain. The deceptive qualities can facilitate manipulation of data or secret observation of activity, but it can also be used to defend against an intruder by 'allowing' for the intrusion to happen and manipulate the information retrieved. This would result in either harming or confusing the intruder (2015, pp. 336–7).

Meanwhile, Borghard et al. (2019) argue that the reason why we have not yet witnessed any of the alarmist scenarios of the cyber escalation literature is because cyber operations are unsuited as escalatory tools. This is due to four mechanisms: Firstly, the retaliatory capacity may not be available when needed because they take time to make and are transitory in nature. Secondly, their effects are uncertain, often limited and reversible. Thirdly, deploying offensive cyber operations demand tradeoffs for policy makers, which sparks hesitancy. Finally, escalating out of domain to a kinetic attack is unlikely to be chosen as an option because of the "limited cost-generation potential of offensive cyber operations" (Borghard and Lonergan, 2019, p. 122). The authors argue that the fear of a preemptive strike, often highlighted among some policy practitioners[5] and scholars, is unwarranted for these reasons and point to the empirical record of activity in cyberspace remains predominantly at the 'nuisance level' and tends to be responded to in a tit-for-tat fashion (p.123).

Fischerkeller and Harknett (2019a) answer the same question by pointing to the strategic value of cyberspace being dependent on it remaining a peaceful domain. The authors argue that states can obtain strategic effects through cyber campaigns, defined as coordinated cyber operations deployed in sequence over time that create strategic advantage through "cumulatively enhance one's own power or degrade and destabilize others' sources of national power" (2019a, p.274). Since

[5] See Clapper et al. (2017) for an example.

advantage can be gained short of war, the authors hold that using cyberspace for attacks comparable to kinetic violent attacks in effect "overshoots the strategic utility of cyber operations" (2019a p.274-5). This would entail that states are *incentivized* to keep their activity within a space that will not risk outcomes that may jeopardize the peacefulness of the domain. Launching an operation that escalates out of domain may prompt cross-domain retaliation and see a new dynamic emerge and alter estimates of interests, risks, cost and challenges (Fischerkeller and Harknett, 2019a, p. 274). Harknett and Smeets (2020) support the view of strategic effects cumulating through low severity cyber operations. They also hold that states are incentivized to keep their cyber operations at low intensity and severity because such activities are more difficult to detect and sanction due to immature international norms and often unclear national legislation on the area (Harknett and Smeets, 2020, p. 12).

A central bias that fueled the view of cyber operations being inherently escalatory was the emphasis on *theoretical possibilities* over the empirical record. Another bias has been connected to what should be considered a *strategic* effect of importance. Much of the literature on strategy in cyberspace has been overtly focusing on the coercive value of cyber operations because this has been seen as the towering strategic aim obtainable through the domain. The following section will examine the empirical record on the coercive value of states' cyber operations.

2.3 The empirical record on coercive value

It has been pointed out earlier in this study how the debate on the importance of cyberspace has been preoccupied with the coercive value of cyber operations (Lindsay and Gartzke, 2016; Whyte, 2016; Hodgson *et al.*, 2019). Several of these studies focus on single high profile cases, such as the Stuxnet worm targeting the Iranian nuclear plant in Natanz (Langner, 2013; Lindsay, 2013; Zetter, 2015) and the North Korean Sony Pictures attack in 2014 (Whyte, 2016; Sharp, 2017). Yet, if one considers the totality of the cyber operations deployed by states, there have been comparatively few publicly known instances of cyber operations as effective coercive tools. The function of studies of single high profile cases tend to be advancing an understanding the *extremities* of the potential in cyberspace, with the aim of determining the outer edges of the room to maneuver. This overemphasis on the *theoretical potential* in the domain distracts us from advancing an understanding of the different forms of utility of the operations that make up the majority of the inter-state activity in the cyberspace.

Recent empirical studies have cast a wider net for understanding how cyber operations are *actually* used between dyads of adversarial states. They have looked at the *total* of the cyber operations deployed by adversaries in dyads sampled form a variety of contexts and regions. These studies have created fertile ground for advancing the scholarship from an emphasis on exceptional cases and theoretical potential to a more thorough understanding of the actual empirical record. Valeriano and Maness (2014) examined the dynamics in cyberspace between adversaries between 2001 and 2011 and found that the activity was restrained in nature and rare in occurrence (p.359). Valeriano et al. (2018) tested the coercive value of cyber operations by examining 192 episodes of cyber operations between rival states from 2000 to 2014 and their effectiveness in obtaining concessions. With the starting point of the three cyber propositions detailed by Rid (2012) of *subversion, sabotage* and *espionage,* they found that cyber operations in general have little coercive value, with only 5.7% of the cyber operations they studied producing an observable concession (2018 p.17). In addition, all the 5.7% were deployed by the United States, which begs the question of whether the same operations would have had equal coercive effects if deployed by a state not towering most measurements of conventional power. Valeriano et al. (2018) found identified three propositions in their analysis – *disruption, espionage and degradation* – of which only *degradation*[6] was deemed coercive in nature, while the two remaining strategies were overall used to "shape future interactions and limit escalation more than they do to seek concession in

[6] Defined as "high-cost, high-pain efforts that seek to degrade or destroy critical capabilities through computer networks" (Valeriano et al. 2018, p.41).

the present" (2018 p.78-83, 3). The tit-for-tat dynamic of retaliation within domain is commonly accepted in the scholarship, and was also confirmed by Valeriano et al. (2018). Their research found that the vast majority of their dataset consisted of low-severity operations that sparked a single response within the same domain. This response did not escalate the tension in the relationship of the adversaries in question. They concluded that the cyber operations therefore may be seen as a stabilizing dynamic that aids the parties in avoiding escalations in other domains instead of as a coercive tool (2018, pp. 76, 88).

A question that emerges from the scholarship discussed above is why the study of non-coercive cyber operations is so absent from the literature. This can be answered by looking toward the general view of what is considered an outcome of strategic importance for policy. This author holds that coercion is emphasized in the literature on this topic because it is viewed as the chief way to achieve outcomes of strategic value. This may be tied to the fact that it has often been the military branches of states that developed the *offensive* capability of deploying cyber operations. This, in turn, may explain the bias as described by Harknett and Smeets (2020, p. 1) as "to consider 'war' as the only critical concern and thus the debate over whether a cyber operation on its own can constitute war appeared as the key issue to resolve". The following section will discuss approaches to understanding non-coercive cyber operations in a strategic space short of war and elaborate on approaches to understanding the potential *strategic effects* or *strategic usage* of this activity.

2.4 Non-coercive cyber operations in the strategic space short of war

The strategic space short of war, broadly defined, encompasses all state interaction short of open military confrontation. This includes coercive strategies such as compellence and deterrence. Coercion strategy "relies on the threat of future military force to influence an adversary's decision making but may also include limited uses of actual force" (Byman and Waxman, 2002, chap. 1). A synonym to this term is *sub-threshold activity*, which is often found in the literature on hybrid warfare to describe coercive action that remains at a distance from a threshold, the crossing of which would merit a clear response from the adversary (Takahashi, 2018, p. 795). Grey zone strategies, in turn, exploit the spaces in between established thresholds to make it politically difficult or even irrational for an adversary to counter the activity (Takahashi, 2018, p. 795). Cyber operations fall neatly within the group of well-suited tools for grey zone strategies by virtue of their relative anonymity and lack of violent first-order effects. For the purpose of this study, the strategic space short of war for cyber operations will be understood as "inclusive of an above operational restraint (i.e. inactivity) and exclusive of an below operations generating armed-attack equivalent effects" (Fischerkeller and Harknett, 2019a, p. 273).

One entry point for understanding non-coercive use of cyber operations within this strategic space is the debate on whether this activity is best understood as an *intelligence contest.*[7] Rovner (2019) defines the intelligence contest in cyberspace as consisting of five elements:

> *"First, it is a race among adversaries to collect more and better information. Second, it is a race to exploit that information to improve one's relative position. Third, it is a reciprocal effort to covertly undermine adversary morale, institutions, and alliances. Fourth, it is a contest to disable adversary capabilities through sabotage. Fifth, it is a campaign to preposition assets for intelligence collection in the event of a conflict"* (Rovner, 2019).

Rovner's definition illustrates how core activities of intelligence organizations overlap the central functions of cyber operations. A central question in this debate is whether the deceptive practice of intelligence can work at scale. Fischerkeller et al. (2020) argue that deception loses its effectiveness when scaled, and consequently that the intelligence contest-thesis falls. Lindsay (2020) is more split in the question and points out that covert action[8] typically is used on the margins

[7] The participants in this debate recognize that there is no agreed upon definition of intelligence. See Warner (2002) for a debate on the issue.

[8] Covert action is defined as "the effort of one government to influence politics, opinions, and events in another state through means [that] are not attributable to the sponsoring state" (Anderson, 1998, p. 423)

to tip events in one or another direction, and not at scale for larger strategic impacts. However, he points out that discreet surveillance, dissimulation and tactical surprise conducted in or through cyberspace overlaps with classical intelligence activity. Warner (2019) argues that although covert action has traditionally been applied ‘on the margins’, the ability of conducting them at scale through cyberspace opens the door for accumulated strategic gains. Warner’s conclusion is supported by Harknett and Goldman (2016).

Harknett and Smeets (2020) are not approaching the topic as an intelligence contest but argue that non-coercive cyber operations can result in strategic effects. They argue that the use of cyber operations over time is *strategic* in its intention because it is consciously aimed at creating a shift in the relative power between states (2020, p.19). Cyber campaigns may, in their view, “turn two initially symmetric relations to asymmetric relations - and vice versa - due to loss of innovation and productive capacity” (Harknett and Smeets, 2020, p. 10).

Other scholars support this claim. Fischerkeller and Harknett (2019a) argue that the interconnected nature of cyberspace opens the door for states to compete robustly short of war over relative gains, and that this creates an incentive to remain in this space and avoid escalation. They refer to the US strategy documents of 2018 for support, which state that US adversaries are working to gain advantages militarily, politically and economically thought strategically deployed cyber operations (The White House, 2017a, p. 3; Mattis, 2018, p. 2; United States Department of Defense, 2018, p. 1). Fischerkeller and Harknett (2019b, 2019a) argue that this entails that persistent campaigns conducted in cyberspace below a threshold for an armed attack *can* create cumulative strategic advantage. Gartzke and Lindsay’s (2015) deception strategy connects to this stance as well. The strategic effect of cyber operations would in their view not be tied to the *direct* effects of cumulative effect over time, but a successful deception strategy would over time increase the competitive strength of its wielder, resulting in strategic advantage.

The above discussions of strategic effects of cyber operations focuse on the long lines of state competition. This does not necessarily overlap with the utility of the operations in the short-term dynamic of adversarial relationship. The following section will discuss key debates regarding a central function of cyber operations in the strategic space discussed; namely their signaling value.

2.4.1 Ambiguous communication

In their large empirical analysis of a decade of cyber operations between adversaries, Valeriano et al (2018) found that the operations often were used as signaling tools. However, the message communicated by a cyber operation can be a challenging thing to dissect. Borghard (2018) points out that there appears to be no common understanding among major cyber powers as to what cyber operations signal to the victim state. With cyber operations being dependent on stealth in order to be effective, the question arises if the operation is meant to remain secret, which would suggest that no signal was intended.[9] Borghard (2018) uses the example of Russian penetration into critical infrastructures of the US. This penetration may be a signal of capacity but meant to advance a deterrent strategy. It could alternatively signal an intent to actually disrupt critical infrastructure in the event of a conflict. Not knowing what part of the state structure is behind the operation also obscures the real meaning of the signal. Whether the intrusion was carried out by the military branch, civil intelligence or private companies communicates a great deal of the potential aim of the operation, and consequently, how the victim state should read the incident.

There is a debate on whether one should look to the *effects* of an attack or to the *effort or means* deployed when designing a response. Proponents of the *effects*-school generally hold that in the cases where the effects are comparable to that of the conventional domains, the policy responses should be equally alike (Rid, 2012; Gartzke, 2013). Proponents of the opposite camp argue that since there are qualitative differences to cyber 'weapons' and conventional weapons, the two

[9] Recent scholarship has disputed the claim the covert operations, by virtue of being intended to be secret, do not hold signaling value. This will be expanded on later in this chapter.

classes would have different policy responses (Farrell and Glaser, 2016). This camp points specifically to the behavioral and psychological effects of different weapons. “The virtual nature of the domain, the high uncertainty of attack, and the machine-centered focus of cyberspace operations may mean that human beings respond qualitatively differently to cyberspace operations than operations in physical domains” (Kreps and Schneider, 2018, p. 12). Whereas a nuclear attack would spark a fight or flight response, cyber operations would likely create anxiety and confusion.[10] Smeets (2018b) expands on how the psychological effect “could be both the main purpose and side effect of using an offensive cyber capability” (p. 102). Smeets (2018b) discusses further how the most prominent psychological effects of offensive cyber operations tend to fall into the subtle category of humiliation and confidence degradation, as opposed to the more explicit conventional effects of fear. “It is also less about threatening escalation and more about *exposing vulnerability* for offensive cyber operations” (Smeets 2018b, p.101, emphasis added).

Libicki and Tkacheva (2020) continue down the same track when discussing how a core challenge of using cyber operations in armed conflict is the ambiguity of how it is to be *read.* Interpreting intent into an action can often prove difficult, but is especially so in the realm of cyber (Lin, 2012b, p. 53). Libicki and Tkacheva (2020) point to how the one and same operation can be understood as preserving the status-quo according to one rationale, but escalatory according to another. The non-lethal outcomes of a high impact cyber operation launched at the homeland of a state in limited conflict with another may be de-escalatory because of the non-lethal outcome, compared to the potentially lethal effects of a continued military advancement. The same operation could also be seen as escalatory since it *moved* the impact to the national territory of the state (2020, p.62-4). The authors further point to the challenge that cyber ‘war’ is understood and experienced very

[10] Kreps and Schneider (2018) reveal that the states falling victim to cyber operations from adversaries are surprisingly tolerant of these attacks. The authors find that states seem to refrain from escalating the level of conflict as a result of a cyber attack, even when the effects are comparable to those of conventional or nuclear attack.

differently by various parties. One side can frame a cyber operation as launching havoc on the adversary, whereas:

> *"[t]o 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 fire, but on the other side, cyber war adds complication but not necessary catastrophe."* (Libicki and Tkacheva, 2020, p. 67)

The same action can therefore communicate different messages to different audiences, depending on the framing of the sender.

Covert nature is a central quality of cyber operations that has only been lightly touched upon so far in this chapter. This complicates the communicative value of cyber operations. However, the scholarship on covert action offers valuable insight into this aspect of cyber operations as tools for policy. Carson (2018) has documented how the use of *covert* action facilitates a space for tacit bargaining between the parties engaging in war, particularly by mitigating the pressures from domestic hawks on both sides, therefore limiting escalation. Additionally, he found that working covertly facilitated the wish to 'preserve diplomatic legitimacy', a crucial part to building international coalitions in support of a war. Warner (2019) described the rationale in the following way:

> *"In short, given modern strictures* [sic] *on aggressive war, a state gains more allies for its preferred policies and allies* [sic] *if its behavior is viewed as following international law and norms—and if the behavior of its opponents is seen as violating them"* (Warner, 2019, p. 34).

Brantly (2016) plays along the same lines when he divides overall policy into three groups; "(1) non hostile overt bargaining, (2) hostile overt bargaining, and (3) hostile covert action" (2016, p.18). He argues that the last group is the one that is the least discussed in the International Relations literature, and the one that is the most used in cyberspace. Hostile covert action is also a class of policy that does not include the open sacrifice of political capital, as opposed to the former two groups (2016, p.18). This aspect is interesting because it may incentivize resolving to this segment of policy, if the aim is obtainable through covert means. Carson and Yarhi-Milo (2017) have greatly advanced the understanding on the signaling power of covert tools of statecraft. In this work, the authors show how the perpetrators' involvements are more 'open secrets' to the victims of covert operations since states typically signal their preferred outcomes and communicate their red lines well. Cormac and Aldrich (2018) presented the needed presence of *implausible deniability* on claims of involvement. The eventual deterrent value of the operation would be dependent of the perpetrators denials of involvement being *implausible.* There is a striking parallel to cyber operations on this point, which counters the claim by Borghard (2018) that secret policy tools carry no intended signaling power.

2.5 The role of cyber operations vis-a-vis conventional policy tools

The use and usefulness of cyber operations have traditionally been studied in isolation from the other tools of statecraft available to a state. However, some scholars have alluded that cyber is *most likely* used in concert with other tools of policy to obtain the desired result (Byman and Waxman, 2002; Gartzke and Lindsay, 2015; Valeriano, Jensen and Maness, 2018, chap. 3). Valeriano et al. (2018, p. 99) point to how *combined strategies*, where cyber operations are combined with conventional foreign policy tools, are likely what states practice in reality when attempting to obtain a desired outcome. However, the authors here refer to *coercive* effect of the operations. Valeriano et al. (2018) have also pointed out that cyber operations seldom have a significant impact on their own, and most often "act as additive measures that amplifies existing signals" (2018, p.23). Some have also pointed to the role of cyber in modifying other conflict processes, while still emphasizing the coercive effect, and with the object of study being *one* large cyber operation (Lindsay, 2013; Lindsay and Gartzke, 2016; Whyte, 2016). However, it is assumed that states use their arsenal of policy tools in a strategic manner to obtain the desired results, also in situations when they do not want to coerce. Jensen (2017) argues that cyber operations are useful tools of sub-crisis maneuvering because they offer an option for policy when other tools appear unfitting. Jensen and Valeriano (2019) see cyber operations as fruitful escalation offramps, detailing that “[e]ven states with more escalatory attitudes tend not to respond militarily to disputes when they have the option of imposing costs and signaling through cyberspace” (2019, p.2). This gives them a specific role in the arsenal of policy tools a state posits.

This author aims to fill a gap at the intersection of three central critiques of the literature on the utility of cyber operations and their impact on state interaction. The first point is the emphasis on cyber operations as eventual *instigators* of escalation. This study expects to see how cyber operations are used as a response to escalatory moves by an adversary, although not leading to escalations themselves. The second point is the implicitly held claim that coercive effect of cyber operations is the only strategic importance for states. This study expects to see that non-coercive cyber operations are aiding states in advancing their strategic goal. Thirdly, that cyber operations are too often studied in isolation from the remaining policy tools of the state. This author believes this approach is missing in the study of cyber operations as tools for policy. In order to get a better understanding of the usefulness of cyber operations, one must examine what role it is given in relation to conventional policy tools.

Chapter 3 - Research design and methodology

3.1 Introduction

This chapter will outline the research methods component of this study. This author adopts a research strategy of a case study of one state’s comportment toward another within the context of a long-term hostile feud. Within the case of this feud, the use of cyber operations will be analyzed as an embedded subunit of study for an explanatory qualitative analysis. The empirical research component of this study will create a foundation for the following analysis, which is needed to provide validity for the study. Furthermore, the data collected include the parameters, targets and effects of offensive cyber operations conducted by Iran against the United States in the timeframe July 2015 through 2020 and will be compared to Iranian usage of conventional policy tools. Finally, information about the development in the context of relevance to the case and Tehran's top strategic goal also needs to be collected.

These three components – use of cyber operations, conventional policy tools and the development in the relationship – are needed to show if there is a pattern of behavior that may shed light on *the role* of Iran's cyber operations vis-a-vis the conventional tools at its disposal.

This chapter will set out by outlining the research strategy of this study and present the rationale for methodological choices. It will then continue to explain and define the case to be examined, then map out the process of data collection, before presenting the theoretical framework for analysis. At its close, the chapter will detail limitations of this study and potential problems that the author may encounter in the prospect of its completion.

3.2 Research strategy

The objective of this study is to nuance how cyber operations are used vis-a-vis conventional policy tools in a non-coercive manner in the strategic space short of war, applying an explanatory case study with Iranian cyber operations as an embedded unit of study.

The research question of 'what is the role of cyber operations in Iran's policy toward the United States?' will be answered through a two-step analysis. The first step will test the hypothesis "the cyber operations will follow the escalation dynamic in the other domains" to be answered through a simple pattern-matching of the Iranian activity in the political and military domains and the development in the context. This step should help indicate if the activity in the cyber domain changes quantitatively or qualitatively is in accordance with the development in the context and the Iranian activity in the political or military domains. It should also shed light on under which circumstances Iran uses its cyber operations. Since the relevant literature fails to detail how this pattern should manifest itself, this author works under the assumption that when a state sees a top strategic interest being challenged, it would use all the available tools at its disposal to secure its most vital interest. As it has been explained in the preceding chapter, the study wants to test the assumption that Iran deploys cyber operations to advance its strategic aim in a non-coercive way and do not lead to significant escalation in the other domains (Valeriano, Jensen and Maness, 2018; Fischerkeller and Harknett, 2019a).

While identifying an eventual pattern of behavior may help shed light on how cyber operations fit into a state's arsenal of tools of statecraft and the utility of cyber operations for advancing a state's interests in a non-coercive manner, the absence of a pattern is also of interest. It may indicate that the state did not consider cyber operations useful for advancing its strategic aim as defined in this study. The second step of the analysis will discuss *how* the cyber operations are useful for the Islamic Republic. It will take a step back and analyze and explain the pattern of behavior detailed above and examine if and how the use of cyber operations would be effective in advancing Iran's power or destabilizing the US' sources of national power. This author assumes that the cyber operations offer some kind of desired effect for the Islamic Republic and aims to shed light on this desired effect from the pattern of behavior detailed in level one of the analysis. By combining the pattern of cyber operations, Iranian conventional policy use and the context within which they occur, this study will advance the understanding of the role of cyber operations in a state's arsenal of policy tools.

According to Yin (2003), "[t]he case study is preferred in examining contemporary events, but when the relevant behaviors cannot be manipulated [...]" (p.7). The approach makes it a good choice for the study of international relations and state interaction, and works as a practical approach to operationalize the study of cyber use by facilitating an in-depth qualitative analysis of the empirical record within one dyad of adversarial states. Denzin and Lincoln (1994) describe qualitative analysis as studying "things in their natural settings, attempting to make sense of, or interpret, phenomena in terms of the meanings people bring to them" (p.2). The way in which states conduct their policy cannot be understood without reflecting on the context in which they emerge. It is therefore pivotal to study this subject through a framework that allows for understanding policy in light of their context to see *how* they are used and *what* they produce. Furthermore, embedded case studies allow examining a subunit of analysis within a wider context of a case (Yin, 2003, p. 43). This approach is therefore best suited to obtain the objective of understanding the *role* of cyber operations in Iranian policy *within* the feud with the US. Yin (2003) identifies a pitfall when conducting embedded case studies if the researcher "focuses only on the subunit level and fails to return to the larger unit of analysis" (p.45). This analysis therefore will return to the case in question by examining *how* the cyber operations aid Iran in advancing toward its strategic aim.

A recurrent criticism of case studies is that they lack generalizability (Yin, 2003, p. 10). This means that the results of the analysis may not be valid outside of the context of the case in question. However, Yin (2003) disputes this claim by pointing to how research designs that aim for *analytical* generalization are able to "expand and generalize theories", citing case studies and experiments as examples of such (Yin, 2003, p. 10). This study will aim at theoretical generalization by building the research design on a sound theoretical footing derived from relevant literature on strategy and policy in cyberspace.

3.2.1 Defining the case study

The case study for this research project has been selected on the basis of its ability to examine the role of non-coercive, non-escalatory cyber operations in a long-term and eventful feud. Iran is an eager user of cyber operations to advance their interests, has steadily invested in its cyber capabilities in the last decade, and is now commonly placed fourth or fifth in offensive capability worldwide, with the United States leading (O'Flaherty, 2020). Since the landmark Stuxnet cyber operation targeting the Iranian nuclear facility at Natanz in the early 2010s, Tehran has conducted several high profile cyber operations against the US and regional adversaries. It is therefore likely that the data collection component of this research will reveal a meaningful number of incidents, facilitating a thorough analysis of the activity. This author's assumption is that Iran will refrain from launching cyber operations of high severity that could lead to a significant escalation in the relationship with the United States. In addition, Iran is expected to make the best use of its cyber operations to advance its position in the feud. Examining *Iranian* use of cyber operations is relevant for the objectives of this research because Iran is the weaker party in the dyad and its activity in this domain is more likely to be representative than that of the outlier topping the sophistication and capability-pyramid in the international system. Cyber operations have become accepted as a tool favored by weaker states, seeing that developing capabilities in this domain demands less resources than conventional military power. Iran is well aware of its inferiority to the United States in conventional military might, and should thus be an illustrative case of states using all tools available short of armed conflict to advance its strategic goals.

The Islamic Republic's feud with the United States is rooted in a long history of geopolitics and Cold War dynamics. The US was close ally of the Shah, which made it a natural ideological foe of the revolutionary movement toppling the Pahlavi dynasty in 1979. According to the narrative of the revolutionaries, the Islamic Revolution eliminated the corruption and immorality of US imperialism imposed on Iran by ousting the Shah. Additionally, the Revolution's role as a liberator from oppression form the imperialist West is rooted in a divine mandate. The ideological foundation of the feud between Tehran and Washington remains static Yet, in a practical sense, the central strategic aim for the Islamic Republic is to exit the economic isolation upheld by Washington by virtue of being the world's largest economy and a super power in the contemporary world order.

For the purpose of this study, the towering strategic goal for the Islamic Republic is being defined as eliminating the sanctions pressure on its economy. This is not just because it would entail economic prosperity and markets for the country's vast oil production and industrial commodities industries, but also because it is tied to the viability of the regime. The sanctions have immense impact on the fluctuations on the national currency and Iranians' freedom to travel. The economic hardship of the sanctions regime has increased the hostility toward the regime and its policies in many segments of Iranian society, sparking cyclical protests and calls for change.[11] Iran has a strong tradition for popular uprisings for voicing dissent and toppling existing regimes. The current regime in the Islamic Republic is painfully aware that itself is the result of such a revolution and harvests much of its legitimacy from this origin. Eliminating an important cause for the population's economic grievances is therefore both a move to ensure increased security for the regime and a means to boost economic prosperity for the state.

3.3 Data collection

This study relies on open-source data when examining the role of Iranian cyber operations toward the United States. Cyber operations are defined as "operations that employ capabilities aimed at achieving objectives in and through cyberspace" (Dinstein and Dahl, 2020, p. 19). This definition includes cyber *exploitation* and cyber-*attack* (Lin, 2012b, pp. 51–2; Brantly, 2016, p. 16). The former class is defined as "[a]ctions taken in cyberspace to exploit information, digital espionage", whereas the latter entail an *active* payload which has an effect on the target (p.16). *Capabilities* are understood as efforts targeting the *CIA-triad*, referring to the confidentiality, integrity and availability of networks, their in-house data or data transfer (Van Puyvelde and Brantly, 2019, p. 57). These capabilities can include different tactics for gaining access and create an effect. Examples include efforts using software to gain access, often through types of malware, such as exploits, worms and backdoors. Other efforts are centered on exploiting the human link through spear phishing campaigns or gaining access to systems through password spraying tactics.

To understand the *role* of cyber operations three sets of information are important. Firstly, available data and parameters of specific cyber operations conducted by Iran targeting the United States; secondly, the parameters of the conventional

[11] Recent examples include the widespread strikes and manifestations in the fall of 2018 (Aziz, 2018), and the vast uprisings in the fall of 2019 against rising fuel prices and general discontent (Fassihi and Gladstone, 2019).

foreign policy tools deployed against the United States; and thirdly, the context within which this occurs. Meanwhile, two variables are relevant to determine the context of the feud: the Iran policy of the United States, and the diplomatic development relating to the Nuclear Deal,[12] including the positions of the other parties to the Deal when this plays into Iran's top strategic aim of relieving sanctions. The last variable group is important because the enactment of the Deal entailed achievement of Iran's central strategic aim, and the decline or eventual collapse of the Deal would reverse the sanctions relief provided by the agreement. Since the activity in the cyber domain is the primary unit of study in this research project, it will be treated as the dependent variable, whereas the context and conventional foreign policy tool-use as independent variables. Again, determining the *role* of cyber operations includes identifying when a state *chooses* to use it to advance its interests. This study builds on the assumption that the use of cyber operations will be deployed as a *supplement* to policy in the political and military domains, which are seen as superior modes of policy.

A list of Iranian cyber operations targeting the United States will be compiled by cross-referencing the open source data repositories on publicly reported cyber incidents monitored by think tanks (Center for Strategic and International Studies, 2021; Council of Foreign Affairs, 2021; Kaspersky Lab, 2021). The data identified will be complemented by further research through examining reports from cyber security companies and news reports. The following criteria are imposed on the data: They must be attributed to Iranian state by either a state body, a cybersecurity company or a news report citing sources with direct knowledge of the matter as a function of their position. The operations must show some relevance to the feud with the United States, either by their direct target, their symbolic nature or strategic importance. This excludes espionage efforts against Iranians living in the United States, the civil sector, and intellectual property thefts from universities and operations conducted by criminal standalone

[12] The official name of the Nuclear Deal is Joint Comprehensive Plan of Action. JCPOA, the Deal, the Nuclear Deal or the agreement will be used interchangeably throughout this study.

actors in Iran.[13] Espionage campaigns spanning across several years will be excluded because they are long-term *strategic* intelligence gathering efforts and not tied to developments in the relationship.

The parameters of the conventional foreign policy tools usage and information on the context for the timeframe studied will be collected through investigating a wide cross section of secondary literature, news reports, analysis pieces and timelines compiled by interest groups and research institutions. Iranian conventional policy tools will be limited to *political* and *military* activity as a simplifying measure. Attempts of political escalation on the part of Iran are altering their policy regarding the nuclear program, while attempts of military escalatory moves are defined as kinetic strikes, military exercises, and tests of ballistic missiles or satellite launch vehicles. The Iranian space program is officially civilian in nature, but the dual use nature of launch vehicles to propel satellites into orbit causes it to be perceived as ballistic missile tests (Pražák, 2021). For the purpose of this study, satellite launches will be classified as a military activity because it is perceived as such by the United States (Schmerler, 2019).

3.4 Framework for data analysis

This study approaches the use of cyber operations in state policy through an escalation-theory lens because it brings with it an empirically suitable conceptualization of the dynamic of action-response between two adversarial states. For the purpose of this study, the relationship between Iran and the United States will be understood as an *agreed battle*, as defined by Herman Kahn (2017). Such a situation emerges between two adversarial states when both sides have a strategic interest not to escalate tensions in the relationship into a military confrontation. An agreed battle implies a tacitly agreed upon *range* of conflict, as well as an understanding of what *behaviors* are acceptable and unacceptable

[13] An example of this is the 2018 ransomware attack against the City of Atlanta's information systems, which was conducted by two Iranian citizens not tied to the Iranian government (State of Georgia, USA, 2018).

within this space (2017, p. xiii). Kahn argues that two ‘classes’ of strategies could be deployed by the parties to an agreed battle. “One class makes use of the factors relating to particular levels of escalation in order to gain an advantage. The other uses the risk or threat of escalation or eruption from the agreed battle” (p.7). The latter class is where coercive strategies such as deterrence, compellence and coercive diplomacy are deployed. The former is where non-coercive interactions occur and describes the strategic space where this study expects Iranian use of cyber operations will occur. However, this author expects that coercive strategies will be deployed by the US against Iran, and possibly by Iran in the political and military domains.

Escalation will be understood as an alteration of a state’s efforts, either in *degree* (intensity/verticality) or *type* (scope/horizontality) (Libicki and Tkacheva, 2020, p. 64). A significant escalation will be considered as having taken place when “at least one of the parties involved believes there has been a significant qualitative change in the conflict as a result of the new development” (Morgan *et al.*, 2008, p. 8). Escalations can happen in small steps, steadily contributing to the level of tension remaining at a certain point.[14] This would entail that the response to a move by one state is equal in severity, reciprocal and is not understood as escalatory to the relationship by the other party. A significant escalation occurs when one party responds to the move of the other party with a move that is higher in severity than the preceding move. This can be done by increasing intensity significantly within one domain, or expand to another domain, as detailed above. According to the theoretical framework at the base of this study, these steps of escalation can be deployed within two different strategic space. In the first, the escalatory moves are used to gain an advantage, while in the other, escalatory moves are used in coercive strategies to threat to erupt from the agreed battle into military confrontation. The division of the strategic spaces therefore indicates a

[14] Libicki and Takacheva (2020) described this as a *horizontal* horizontal escalation, which responds in a tit-for-tat-fashion but remains at the same level of intensity.

move from *competitive interaction* into *coercive interaction* (Fischerkeller and Harknett, 2019b, 2019a).

In order to answer the research question of "what is the role of cyber operations in Iran's policy toward the United States?", two analyses need to be conducted. The first entails examining the pattern of behavior of Iranian cyber operations targeting the United States seen in relation to (1) the development in the context (2) and Iranian use of conventional policy tools. It follows logically from the understanding of cyber operations as a tool of policy available to a state that they should be deployed in some form of pattern reflecting the context and conventional policy use. The literature does not offer a detailed prediction of how this pattern should look, but it follows logically that the cyber operations should follow the dynamic of escalation in the conventional policy use. This shall be answered by testing the hypothesis of "the cyber operations will follow the escalation dynamic in the other domains." This hypothesis will be tested through a chronology-design, which allows for a simple pattern matching of the dynamic of escalation and de-escalation in the context, the conventional domains and the activity in the cyber domain. The pattern identified should help shed light on under which conditions Iran chooses to deploy cyber operations. The timespan of study chosen is from the signing of the JCPOA in the summer of 2015 until the end of 2020.

Five separate context blocks have been defined within this timeframe, partitioned by important milestones or escalation peaks in the relationship. Some context blocks contain several peaks or increases in tensions. The context blocks will facilitate the analysis by dividing the timeframe studied into manageable sizes. The analysis in each context block will be structured as an analysis of the development in the context which details the moves by the United States or the remaining parties to the JCPOA endangering or advancing Iran's strategic goal. This includes introducing sanctions, enacting clauses in the JCPOA and military deployments. Then Iranian policy within this context will be analyzed, divided between political and military moves. The final part of each context block will analyze the Iranian cyber operations targeting the US within the timeframe studied, while placing them within the context and contrast the development to the preceding context block. The Islamic Republic will be analyzed as *one* coherent actor. The Iranian political structure is complex and embossed by corruption. Additionally, the Islamic republic is an eager user of proxy actors. This makes it challenging to form a comprehensive image of which political factions are steering the policy of different branches of the military, civilian and religious institutions. As a simplifying measure, Iranian policy will be treated as *one* entity steered by national interests.

In the second analysis, the insights from the preceding analytical work will help examining *how* the cyber operations contribute to advancing Iran's position in the feud in the timeframe studied. This will be done by taking a step back from the detailed approach of the context-block analysis and look at the empirical structure of context and Iranian policy responses in the entire timeframe studied. The theoretical framework underpinning this analysis posits that states "makes use of the factors relating to particular levels of escalation in order to gain an advantage." (Kahn, 2017, p. 7) Fischerkeller and Harknett (2019a, pp. 274–5) elaborated this framework further by defining 'gaining an advantage' as "increasing one's own power or destabilizing the opponent's sources of national power." This latter definition will be used in this study. Power will be understood as a function of actors' relative placement in the international system (Wendt, 1999). Broadly understood, *sources of national power* entail the structures underpinnings a state's position in the international system. For a democracy, this would include the integrity of its democratic processes, legal system and political structures, but also its reliability as a diplomatic actor and prestige on the international stage.

If a cyber operation of Iranian origin creates a significant escalation in the relationship or appears to be coercive in nature, the assumptions underpinning this study are not valid for this case. If there is no visible pattern of the deployment of cyber operations seen in relation to the escalation dynamic in the context and

Iranian conventional policy tools, the hypothesis will be considered falsified. This would indicate that Iran does not use its cyber power to advance its interest directly vis-à-vis the United States. This may be because it does not consider cyber operations a tool of policy that is fitting for the aim in question, or that it chooses to prioritize its efforts differently. Regardless of the motivation for non-deployment, it may suggest that cyber operations play no active role in advancing Iran's position in the feud with the United States.

3.5 Methodological reflections

Several methodological limitations have been identified to this research. First, this study examines only one state's cyber operations and does not systematically look at counter-operations by the United States or its allies. Second, this research will lean primarily on English language sources. Access to Persian sources would have provided a more complete image of the dynamic from Tehran's point of view. This challenge is mediated by making use of English language Iranian scholarship and Iranian news outlets with English language.[15]

Furthermore, reliability will be ensured through a replicable and transparent research structure and thorough referencing. Certain limitations follow from studying cyber operations in particular. Yin (2003) points out that a research project will have to "[d]emonstrate that the selected measures of these changes [being studied] do indeed reflect the specific type of change that have been selected" (p. 35). This is challenging to establish with high certainty when the subject of study is cyber operations because of the covert nature of the activity, the relative anonymity afforded to the actors and the way in which they are reported and attributed. This issue has been discussed at length in the literature (Lindsay, 2015; Rid and Buchanan, 2015; Edwards *et al.*, 2017; Egloff and Smeets, 2021). Intelligence organizations and cybersecurity companies undoubtedly have a more complete image of the scope of activity but are unwilling to share this information due to national security or private industry

[15] Examples include Islamic Republic News Agency (IRNA.ir), Tasnim News Agency (tasnimnews.com) and The Tehran Times (tehrantimes.com).

interests. However, as with all studies of cyber operations, this project will have to rely on publicly available data.

There is also a temporal challenge with studying cyber operations. It follows logically that a move from one actor will be a response to a move by the other actor when it follows it closely in time. Cyber operations are somewhat complicating this due to different temporal parameters than other policy tools. The time required to prepare an operation varies greatly with the sophistication of the operation and its design. Therefore, the decision to engage an operation may have been made months before it is deployed, which complicates attaching an operation to a specific context and escalatory move. This challenge is mediated by the use of context blocks spanning between seven and 18 months in time, established after the most significant milestones in the relationship. This move helps overcoming the temporal issue by examining large timeframes. Also, when available, the information on the start time of the operation will be included, which facilitates tying it to an eventual specific move or development.

Chapter 4 - Data analysis

This chapter will undertake the empirical analysis of this study, in which the first part will analyze the state dynamic in the relationship, Iranian policy responses in the political and military domain and Iranian cyber operations targeting the United States. Three major escalation milestones emerge during the timeframe studied, as well as several of relatively less severity. In level two of the analysis, this author will put forth empirical findings from the pattern matching in level one before analyzing and discussing the wider correlations shedding light on the role and utility of the cyber operations for Tehran.

4.1 Pattern matching and hypothesis testing

4.1.1 July 2015 to November 2016: The JCPOA – US presidential elections

The long diplomatic effort to reach a diplomatic agreement that would dismantle much of the Iranian nuclear program and open its nuclear facilities to international inspections in exchange for inclusion into the global economy was concluded in the summer of 2015. The Joint Comprehensive Plan of Action (JCPOA) was developed and upheld by Iran, the United States, France, the United Kingdom, Germany, China, Russia and the EU. This introduced a historic level of goodwill in the relationship between Iran and the United States. Through the summer and early fall, the JCPOA was passed by the US and Iranian legislators, while resolution 2231 endorsing the Deal was passed unanimously in the UN Security Council. The United States followed the steps detailed in the Deal, gradually relieving sanctions. This resulted in lifting restrictions on sales of aircrafts to Iran, as well as sanctions on the oil and financial sectors, and releasing frozen assets in foreign banks belonging to the Iranian state (Jaffe and Mufson, 2016; Sanger, 2016).

In this first time period, Tehran was steadily de-escalating in the political domain through gradual compliance with the requirements of the JCPOA. Iran met every deadline to comply with the obligations from the Deal, testified to in all IAEA's reports (Director General IAEA, 2016a, 2016b, 2016c, 2016d). The only inconsistency was two instances of small breaches of the cap on the allowed stockpile of heavy water. In ratifying the JCPOA, Iran agreed to implement the Additional Protocol of the Non-proliferation Treaty, which assured IAEA inspectors access to Iranian facilities for inspection (Director General IAEA, 2015). This was a period of diplomatic and reputational success for Tehran, advancing steadily toward the desired outcome: relief of all sanctions. Tehran additionally enjoyed a position it had seldom held in previous decades. By entering into the JCPOA, Tehran was in the diplomatic company of the major powers in the international system.

Meanwhile, Iran conducted a parallel increase of activity in the military domain, notably tests of three types of ballistic missiles. On October 11, 2015, Iran tested the Emad long-range precision missile (Hume, 2015; Wilkin, 2015), while one Ghadr-1 medium-range ballistic missile was tested in November 2015 (Charbonneau and Nichols, 2015). The US criticized the first launch in the UNSC in October 2015, claiming they were in breach with UNSC resolution 1929[16] because Washington considered the missile capable of carrying a nuclear warhead (Charbonneau, 2015). The US proceeded by issuing sanctions on 11 individuals and entities connected to the ballistic missile program in January 2016 (BBC, 2016). Resolution 1929 is widely interpreted by Western powers to contain a prohibition on all ballistic missile tests for Iran (United Nations Security Council, 2010; Davenport, 2017c). The same applies for resolution 2231. The official Iranian response does not recognize any restrictive measures on its ballistic missile program, which it holds is essential for its self-defense. Tehran further holds that the wording of resolution 2231 does not constitute a ban, as it is "calling on" Iran to refrain from ballistic missile activity that includes a capability to deliver nuclear warheads (United Nations Security Council, 2015, p. 99; Davenport, 2017c). Moreover, Iran's largest military escalation in the first year following the Deal was the early March 2016 test of two short-range ballistic missiles of the types Simorgh 1 and 2, as well as two Ghadr-1 medium-range ballistic missiles (Mostaghim and McDonnell, 2016). The US response was measured, with the Obama administration deeming them 'provocative', though not a breach of the JCPOA (Mostaghim and McDonnell, 2016). Iran also tested its then largest satellite launch vehicle on April 19, 2016, although the success of this test is uncertain. The Simorgh launch vehicle was developed for propelling satellites into orbit, while it is considered by the Pentagon to be central to the development of long-range ballistic missiles. The Simorgh also has enough lift power to carry a nuclear warhead, according to US officials (Eshel, 2016). Two

[16] Resolution 2231 replaced the 1929 resolution when it entered into force on January 16th 2016 (Davenport, 2016). This is why the October launch was seen as a breach to 1929, whereas the later launches were considered a breach of resolution 2231.

more missiles were tested, one in July and one in September that same year (Times of Israel and Associted Press, 2016; Mizokami, 2017; Iran Watch, 2020).

The Iranian missile tests and the US diplomatic responses were, nevertheless, a parallel to the continued advancement of the implementation of the JCPOA, and it did not appear to be severe enough to prompt escalation of importance in the relationship. The US was aware that Tehran did not consider itself bound by any restrictions on its ballistic missile program. The ballistic missile tests occurred with a steady interval and did not appear to be connected to any particular move by the Unites States.

4.1.1.1 Iranian cyber operations

During this period, Iranian cyber operations were almost absent from the interaction in the relationship. Only one incident was included in the dataset for this study, of a total of 15 entries. In November 2015, several government officials at the US State Department (USSD) working on Iran-related issues had their social media and email accounts hacked (Sanger and Perlroth, 2015; Solomon, 2015). The aim of the operation seemed to be reconnaissance on persons of interest, with media accounts alluding to the reluctance of some factions of Iranian political power centers, the IRGC[17] in particular, to the opening of the economy to foreign investments and economic activity (Solomon and Fassihi, 2015). This would make this cyber operation in question an outlier in regard to the core of the feud as defined for this study, since it opposes the overall aim of economic inclusion for the Islamic Republic.

4.1.2 November 2016 to May 2018: Presidential elections – The US JCPOA exit

With the entry of a new administration came a shift in tone from Washington. President elect Donald Trump had been a vocal opponent of the JCPOA through his candidacy and pushed for a new and more far-reaching deal that would restrict

[17] The Islamic Revolutionary Guard Corps is a military branch under the authority of the Supreme Leader. IRGC will be used interchangeably with Revolutionary Guard.

the nuclear program further, have a longer timeframe and include the Iran's ballistic missile program and regional activities. Efforts quickly emerged from Congress aimed at ramping up the pressure on Iran. In December 2016, Congress renewed the Iran Sanctions Act (ISA) and in March 2017 a new and more far-reaching sanctions bill, dubbed the Countering Iran's Destabilizing Act, was presented to Congress by Senator Corker. The Corker bill was passed by the Senate in June and incorporated in the Countering America's Adversaries through Sanctions Act that was signed into law in August 2017 (Corker, 2017; Royce, 2017). The text of these bills had been adjusted not to be in breach with the US obligations in the JCPOA, but it would nonetheless increase the sanctions pressure on Tehran. The European parties to the JCPOA urged the US to refrain from actions that would endanger the Deal and spoke out on several occasions in support of it.

Parallel to the new legislation, the Trump administration upheld the JCPOA on paper but took steps to counteract its implementation in informal ways. During the G20 Summit in the summer of 2017, President Trump encouraged foreign leaders not to increase their business dealings with Iranian companies, a core component of the JCPOA (The White House, 2017b). The administration delayed the certification of Iran's compliance with the Deal in July and paired this with announcements of new sanctions on the ballistic missile program and procurement of materials for missile production (United States Department of State, 2017). These sanctions were tied to an alleged purchase of materials for ballistic missile production by the Iranian military, revealed in June 2017, though it may have taken place in October 2016. [18] The United States argued on the base of this event in favor of the JCPOA being replaced with a more comprehensive deal. The administration issued additional sanctions on the IRGC for support of terrorism the same month (United States Department of State, 2017). In a shift of official stance, President Trump announced a new strategy on Iran in October

[18] Such a purchase falls under the arms embargo on Iran established in Resolution 2231, which holds that a the UNSC shall be informed and give a green light in the case of Iranian import of materials that may be used for ballistic missile production. (Davenport, 2017b).

2017. The administration would stop certifying Iran's compliance with the deal, which opened for Congress to re-introduce sanctions within a 60-day window. The administration then put pressure on Congress to take steps to mediate its concerns regarding the timeframe of the JCPOA and Iran's ballistic missile program. Through the spring of 2018, the Trump administration conducted a diplomatic push for a supplemental deal on Iran but was met with resistance from the remaining parties to the JCPOA.[19]

4.1.2.1 Iranian policy

In this period of increasing pressures, Iran continued a strategy of overall de-escalation in the political domain through compliance with obligations from the JCPOA. IAEA certified compliance in all quarterly reports (Director General IAEA, 2016e, 2016f, 2017a, 2017b, 2017c, 2017d, 2018d). In the wake of the announcements of new sanctions legislation from Congress, Iran signaled its discontent in different ways, but did not take steps that countered the JCPOA. After the renewal of the ISA in December 2016, President Rouhani announced a research and development program on nuclear propulsion for marine vessels (Fitch and Eqbali, 2016). It is unclear whether this project entailed enriching uranium at high purity-rates, as some designs of such vessels require 90% purity and others 10%. Nevertheless, the announcement was scarce in detail on the development track, and little information about the project was shared in the following year. Only in February 2018 did the IAEA confirm that Tehran had informed them of the intent to pursue such projects in the future (Director General IAEA, 2018d, p. 5). The announcement of the Countering Iran's Destabilizing Activities Act in March 2017 and the bill it became a part of and signed into law the following August were met with verbal condemnation by Iranian authorities. The latter was described by President Rouhani as a 'clear hostile act' (SBS, 2018). Meanwhile, Iran increased tensions in parallel through *marginal* escalatory

[19] There was a slight split in the European stance. The EU's then High Representative for Foreign Affairs and Security, Federica Mogherini, stated that the EU was not considering sanctions on Iran's ballistic missile program, while French President Macron stated that he agreed to work with the Trump Administration towards this aim (BBC News, 2018b).

actions in the military domain. The case of alleged imports of materials that would be in breach of the arms embargo of resolution 2231 illustrates a marginal escalation in the relationship. Resolution 2231 holds that the UNSC shall be informed and approve Iranian import of materials that may be used for ballistic missile production. This point was re-iterated by the UN Secretary-General Antonio Guterres in his June 2017 report, where he raised concerns over the imports that were confirmed to be of Iranian origin (United Nations Secretary-General, 2017).

During this timeframe, Iran also increased tensions militarily by conducting six ballistic missile tests and one attempted satellite launch.[20] A launch in January 2017 caused the US to designate entities as a response and for the then National Security Advisor Michael Flynn to put Iran "on notice" (Davenport, 2017a; Sanger, 2017). Two more tests were conducted in early March 2017 at the Strait of Hormuz in the Persian Gulf (Chabba, 2017). In late July, Iran conducted a failed launch of a satellite into orbit using the Simorgh launch vehicle. These tests sparked condemnation from the European parties to the JCPOA and the US, with the latter issuing new sanctions targeting entities with central function in the ballistic missile production (Al Jazeera, 2017; Joint Statement of France, Germany, UK and US, 2017). A joint statement by France, Germany, UK and US confirmed that an additional ballistic missile test was conducted on July 4, 2017, while they also condemned six ballistic missiles fired into Syrian territory in June of the same year (Joint Statement of France, Germany, UK and US, 2017). In May 2018, Israel sent a letter to the UN reporting alleged missile tests in January of the same year. Iran rejected the accusations in a subsequent letter (Danon, 2018; Helmhold and Roth, 2018).

4.1.2.2 Iranian cyber operations

Iran appeared to continue its restrained strategy in cyberspace. The dataset displays only one entry in this timeframe. In April 2017, an Iranian hacking group

[20] In the summer of 2017, Iran launched six ballistic missiles into Syrian territory as part of the military engagement against the Islamic State. These are exempt from this study.

attempted to gain access to the network of a US military contractor. The threat group in question, named APT 34 or OilRig after its history of targeting Saudi oil infrastructure, used capabilities likely obtained from Russian hackers (Perlroth, 2017). Oilrig is best known for deploying wiper malware on the targeted systems, with the Saudi Aramco operation in 2012 being the most high-profile example. The operation broadly coincided with the advancement of sanctions legislation in Congress and came a month after the ballistic missile tests in March. However, the operation was not particularly significant judged by its target. It was also averted and neither produced known direct effects, nor prompted any response by the US.

4.1.3 May 2018 to May 2019: US JCPOA exit – Iran's decrease in compliance

May 8, 2018, marked the first significant escalation in the relationship between Iran and the United States in the timeframe for this study. President Trump's decision to exit the Nuclear Deal introduced a gradual re-introduction of the pre-2015-sanctions after a 'wind-down' period of 90 days for some sanctions, and 180 for others (United States Department of State, 2018a; United States Department of the Treasury, 2018). The US exit introduced the Maximum Pressure campaign, a coercive campaign aimed at changing *regime behavior* in Tehran, particularly in regard to engagement in the region and the ballistic missile program. US Secretary of State Michael Pompeo issued 12 demands to Iran that had to be met before negotiations over a new deal could take place (Annan, 2018). The official US stance sought to establish a more comprehensive deal to replace the JCPOA, which would include the above-mentioned concerns. The first wave of re-introduced sanctions came in the beginning of August 2018, targeting purchases of US dollars and certain metals and commodities. In November, the second round of sanctions followed, targeting Iranian banking, oil, shipping, and shipbuilding. Sanctions waivers were issued to certain countries allowing continued import of reduced levels of Iranian oil and for cooperation on nonproliferation projects within Iran (United States Department of State, 2018c, 2018b).

Shortly after President Trump exited the JCPOA, European parties to the Deal began intense diplomatic efforts aimed at upholding the agreement and making it economically beneficial for Tehran. This included activating legislation to facilitate European companies' continued dealings with Iran, working on a mechanism for bank transfers outside of the US SWIFT system and issuing economic aid packages (EU Commission, 2018b, 2018a). These efforts continued through 2018 and into 2019. The US Maximum Pressure campaign was coupled with a diplomatic effort to rally support for a more comprehensive deal. On the sidelines of the UN General Assembly in September 2018, the US held a summit dubbed United Against a Nuclear Iran, attended mainly by allies in the Gulf and Israel (United Against a Nuclear Iran, 2018). Attempts to muster support for a new arrangement in the Security Council were countered with statements of support of the JCPOA. The US and Israel also attempted to put pressure on the IAEA to inspect sites they argued housed nuclear material, though without success.

The United States increased the pressure on Iran during the spring of 2019 culminating in a peak in April and May. Firstly, the United States designated the IRGC as a terrorist organization in mid-April (Wroughton and Hafezi, 2019). Then, Washington terminated all sanctions waivers for Iranian oil imports on April 22 2019 and key waivers on nuclear cooperation on May 3 2019. This included the scheme to transfer heavy weather stockpiles and enriched uranium from Iran to Oman and Russia, respectively (United States Department of State, 2019f, 2019a). This move entailed that Iran was unable to continue civil nuclear activity without breaking its obligation under the JCPOA through exceeding the stockpiles allowed by the agreement (Davenport, 2019). National Security advisor John Bolton announced in early May 2019 that the Aircraft Carrier USS Abraham Lincoln would be sent to the Persian Gulf, acting on intelligence that Tehran was planning to engage proxy actors to target US forces in the region (Swan and

Rawnsley, 2019). On the one-year mark of the US exit from the Nuclear Deal, Iran announced that it would gradually step back its compliance with the JCPOA and no longer be limited by the caps on stockpiles of enriched uranium and heavy water detailed in the agreement. A few hours after this announcement, the US issued sanctions on Iranian industrial metals exports, the second largest source of national revenue for Tehran preceded only by oil (Macias, 2019). This was a major blow to the Iranian economy already struggling from the gradual decrease in oil revenues and the corresponding devaluations of the national currency since 2018.

4.1.3.1 Iranian policy

Iran seemingly met the shift in US policy on May 8, 2018, with small escalatory steps within the legal boundaries of the JCPOA throughout the summer of 2018. All the while the regime openly stated that nuclear activities would be restarted if the JCPOA were to collapse (PressTV, 2018). The IAEA continued to testify to Tehran's compliance with the JCPOA in all quarterly reports throughout this period (Director General IAEA, 2018a, 2018b, 2018c, 2019a). Supreme Leader Ali Khamene'i issued seven demands for remaining in the Nuclear Deal shortly after Washington's exit in May 2018. All demands were directed at the European parties to the JCPAO, calling on them to put pressure on the US to cease introducing sanctions, and making an effort to counter the economic losses for Iran that would follow (Tehran Times, 2018). This remained the position of the Islamic Republic throughout the period studied. Iran announced in June 2018 the opening of a centrifuge producing facility in preparation of a 'possible scenario' of the JCPOA collapsing (PressTV, 2018). The Supreme Leader had ordered the preceding day that agencies should be ready to increase uranium enrichment activities. A few weeks later, the Iranian Atomic Energy Organization (IAEO) Chief announced that Iran had built a new facility with capacity to produce up to 60 IR-6 centrifuge-rotors daily (Reuters, 2018). Both moves were technically not in breach of the JCPOA, but were viewed as hostile by the US, although with moderate severity. Tehran also attempted to pressure the US by bringing the withdrawal from the JCPOA to the International Court of Justice in August. Since the US did not recognize its jurisdiction, its ruling in Iran's favor had little effect (BBC News, 2018a; Van der Berg and Sterling, 2018). Apart from these moves, Tehran remained restrained in the political domain until late spring 2019, and it appeared to concentrate its efforts on prompting the European parties of the JCPOA to put diplomatic pressure on the United States to halt re-instating sanctions.

Iran increased the severity of its political escalations significantly in the spring of 2019 through two moves. Firstly, Iran's Supreme National Council quickly followed the US designation of the IRGC as a terrorist organization and designated United States Central Command (CENTCOM) a terrorist organization, effectively deeming the US a "supporter of terrorism" (AP, 2019). In a smaller complimentary move, President Rouhani announced the installment of IR-6 centrifuges at Natanz the following day (Xinhua, 2019). Secondly, the announcement of the gradual decrease of compliance with the JCPOA announced on May 8 was an escalatory move that marked an inflection point of Iran's stance. Up until then, Tehran had painstakingly complied with the provisions of the Deal, which provided the regime political and diplomatic legitimacy. Tehran's statement on May 8, 2018, announced five steps of gradual decreased compliance of the limitations on nuclear activities detailed in the Deal, all of which would be separated by 60 days and would be reversed if the US resumed compliance. The first step was that the stockpile limitations on low-enriched uranium (up to 3.67%) to 300 kg, and of 180 tons heavy water would no longer be respected.

Iran continued cyclical tests of ballistic missiles and satellite launches, provoking condemnations from the US and Europe. In October 2018, Iran fired eight missiles into Syria in retaliation for a terrorist attack against a Revolutionary Guard military parade in the region of Ahvaz that killed 25 and injured 70 one month earlier.[21] In December 2018, Iran launched a medium-range ballistic missile test, which was condemned by the US and the European parties to the

[21] The separatist movement ASMLA (Arab Struggle Movement for the Liberation of Ahvaz) conducted the terrorist attack. The missile strikes targeted militants allegedly supporting the group (Khoshnood, 2021).

Deal (Wintour, 2018). The US and European states continued to hold that Iran breached resolution 2231, which Tehran opposed. On January 15, 2019, the Simorgh space launch vehicle was tested once more in a failed satellite launch. The US continued to protest each launch and advocated for a wider Deal (Schmerler, 2019). On the 40th anniversary of the Islamic Revolution in early February 2019, Iran conducted the first known test of a new type of long-range cruise missile (Al Jazeera, 2019a; The Defense Post, 2019). A few days later, Iran silently conducted another satellite launch attempt with the Simorgh vehicle, which appeared to be a failure (Clark, 2019). Although the diplomatic and political responses to the tests and launches were starker than before, the pattern remained the same as earlier, with cyclical tests at steady intervals. However, the number of tests were fewer now than in the few preceding years, potentially to avoid giving the US additional reasons to escalate further.

4.1.3.2 Iranian cyber operations

This period showed four instances of Iranian cyber operations against the US, signifying a change in what until then had been a restrained strategy. In July 2018, the cybersecurity company Dragos reported of a global campaign of login credentials theft targeting electric companies (Murdock, 2018). US officials confirmed the operation, which they read as 'laying the groundwork' for an extensive disruption of the electric grid, according to media accounts (Kube *et al.*, 2018). The operation appeared to be probing or attempting to gain access to systems, but with no reports of access obtained to critical systems. US officials stated that nothing suggested a disruptive operation was imminent (Kube *et al.*, 2018). The operation coincided with the first marginal political escalations of Tehran in the summer of 2018. However, news reports noted that several countries in Europe, East Asia and the Middle East were also among the victims (Kube *et al.*, 2018).

In October 2018, individuals in the US government charged with re-instating sanctions on the Islamic Republic were targeted in a spear phishing operation. This coincided with the second wave of re-instating sanctions, but no reports were issued of the degree of success. A wider group of civil society actors, journalists and human rights activists were also among the targets (Certfa Lab, 2018). The private company Citrix, which delivered services to Government bodies and the US military, was breached in December 2018 and March 2019. Six terabytes of data were stolen, but no evidence was found that the operation had led to a breach in US government systems (De Luce and Kube, 2019; Nichols, 2019). In January 2019, a wave of hacking attempts occurred, targeting over half a dozen US federal agencies and several private companies (Perlroth, 2019). These came in the form of intercepting traffic from domain name registrars and using this position to steal login information (Perlroth, 2019). This type of DNS hijacking had been the preferred tool of intrusion in operations targeting 12 countries in Europe, as well as in North Africa and the Middle East (Hirani, Jones and Read, 2019; Perlroth, 2019). There were no reports of breaches or disruptions, but the Department of Homeland Security (DHS) issued an emergency order for entities at risk sometime between late December 2018 and late January 2019, which testifies to its scope. Cyber security company Fire Eye had identified activity of this kind tracing back to 2017, but with a surge in late 2018 and early 2019 (Perlroth, 2019).

The data reveals a pairing of restraint in the political domain with an ending of the restraint in the cyber domain. All the while retaining the diplomatic 'high ground' on the official stage, Iran appears to resume probing activities in cyberspace. Two of the operations appear to have been global campaigns, and only two targeted directly US governing structures. Only one showed a degree of success, although the operation managed to steal data from private companies and not official US systems.

4.1.4 May 2019 to January 2020: Iran's decrease in compliance – Soleimani assassination

The late spring and summer of 2019 was a time of sustained high tensions and several high severity moves by both the United States and Iran. The Iranian announcement of gradual decrease in compliance with the JCPOA set of a series of escalations through the summer and early fall. The United States increased the severity and number of sanctions in this period. Supreme Leader Ali Khamene'i and his office were put on the sanctions list in late June, followed by Foreign Minister Mohammad Zarif one month later. The US accused Iran of attacking two tankers in the Gulf in early June 2019, an accusation the regime denied. The events in the Persian Gulf were severe and created a banding around the shipping traffic in the area. Some states began providing military escort for tankers flying their flag (Axe, 2019). On September 3, 2019, President Trump sanctioned by executive order the Iranian Space Agency and two connected research institutions on accusations of assisting the proliferation of weapons of mass destruction (United States Department of State, 2019c). The following day, a push to curb the financial underpinnings of the IRGC began with a mandate in the designation of the group as a terrorist organization. This effort began by sanctioning several persons and entities participatory in the IRGC's oil export business. Also, the US Treasury issued a Reward for Justice statement offering a bounty for information that could aid in disrupting the Revolutionary Guard's cash flow (USDS, 2019e, 2019d; USDT, 2019). Additionally, sanctions were issued two weeks later on entities suspected for supporting the IRGC financially, including the Iranian Central Bank and National Development Fund (USDS, 2019g). This trend continued in October 2019 when Iran's construction sector was sanctioned due to its economic ties to the Revolutionary Guard (USDS, 2019b).

4.1.4.1 Iranian policy

During this period, the Islamic Republic pursued a strategy of five-step escalation. Every step was announced in advance, at 60-day- intervals and documented by the IAEA, who continued to be granted access to observe and report on Iran's nuclear activities through Tehran's continued implementation of the Additional Protocol. From early June into the early fall of 2019, Iran announced installments of additional centrifuges at Natanz in accordance with the decreased non-compliance with the limitations set out in the JCPOA (IAEA, 2019; Director General IAEA, 2019b, 2019c; Azer News, 2019). Iran breached the stockpile limitation on uranium enriched to 3.67% on July 1, 2019, and the heavy water limit on November 17, 2019.

The second step of the gradual decrease of compliance announced was on July 7, 2019 and consisted of increasing the enrichment degree from the 3.67% cap set by the JCPOA to 4.5% purity (Director General IAEA, 2019d). The third step was set on September 5, 2019, when Iran re-commenced the research and development of advanced centrifuges (Director General IAEA, 2019b; Office of the President of Iran, 2019). Step four took place on November 5, 2019. It entailed enriching activities up to 4.5% at the Fordow facility.[22] This step was of additional significance because the status of the facility was a central point of contention during the drafting of the JCPOA. The security installment of the facility had led the US to suspect it carrying military significance for Tehran. The facility was situated deeply within the mountains and circled by anti-aircraft installments (Gambrell, 2020). As a compromise, the JCPOA prohibited enriching activities at the Fordow facility over a 15-year period. The European parties to the Deal announced that pursuing this fourth step would prompt them to enact the Special Dispute Mechanism in the JCPOA. This would entail an implicit message that Iran was acting in breach with the deal, a red line for Tehran. Tehran went forward with the fourth step despite these threats (Director General IAEA, 2019c).

The steady political escalation of this period was paralleled by a short de-escalation through a rapprochement in October 2019. French President Emmanuel Macron mediated a four-point framework for entering negotiations that had been accepted by both President Trump and President Rouhani. Yet, the attempt to de-escalate collapsed as the Iranians backed out last minute after the US declined a public announcement of lifting sanctions before the dialogue began (Dadouch, 2019; Momtaz, 2019).

On June 20, 2019, Iran engaged in a stern military escalation when the Revolutionary Guard downed a US surveillance drone in the Persian Gulf. This event had a significant effect on the relationship, which up until that point had been centered around political, diplomatic and economic tools. Tehran claimed

[22] Iran announced in the same that it had reached a stockpile of low-enriched uranium at 500 kg, well above the 300kg cap in the Deal (Al Jazeera, 2019b).

that the drone had crossed into Iranian airspace above its territorial waters when it was shot down. This event nearly provoked a military retaliation by the US. Media reports highlighted that President Trump decided to call off a response through limited strikes on IRCG bases shortly before the forces were in position to engage (Abdollah, 2019; Barnes and Gibbons-Neff, 2019; Diamond *et al.*, 2019; McLaughlin, Dorfman and Naylor, 2019). The US retaliated on June 22, 2019 through a large cyber operation, wiping out IRGC databases used for targeting tankers in the Gulf (Nakashima, 2019).[23]

Iran tested a medium-range ballistic missile on July 25 in what appeared to be a calibrated escalation. The missile was launched northward from an undisclosed launch site in the south as to unambiguously *not* directly challenge US presence in the Gulf (Burns and Reichmann, 2019; Schmitt and Sanger, 2019). A failed satellite launch was conducted on August 29, prompting no open reaction of note (Brumfiel, 2019). On September 14, a second important military escalation took place as the Saudi Arabian Aramco oil-processing facilities in Abqaiq were damaged in a drone attack. The United States, Saudi Arabia and the European parties condemned Iran for the attack which had used the Houthi militia in Yemen as a proxy actor. Iranian officials denied the allegations. However, the results of a UN investigation the summer of 2020 evidenced that components of the hard-ware used in the attack were tied to Iran (United Nations Secretary-General, 2020). The US deployed troops to Saudi Arabia as a response to the event and deemed the attack an "act of war". Washington additionally suspended Iranian officials from entering the US, which in practice excluded Iranian leaders from meeting in the UN in New York. Finally, a second cyber operation targeting Iran's ability to spread propaganda was conducted by the United States in late September 2019 in retaliation for the Aramco attack (Ali and Stewart, 2019).

[23] Initial reports defined the target being the control systems of Iranian missile launchers. This was later corrected to be IRGC databases (Nakashima, 2019).

4.1.4.2 Iranian cyber operations

Iran appeared to have increased its efforts in cyberspace in this period, with more targeted operations against US official structures and private companies in the supply chain of industrial control systems. The type of victims are still similar to the preceding context block, but the operations appear to be more focused on strategic targets within the United States and happening more frequently. Over the seven months studied in this context bloc, three cyber operations were deployed. In contrast, the preceding 12 months saw four operations.

Within a few days of the downing of the US surveillance drone and the retaliation by cyber operation, the Director of the US Cybersecurity and Infrastructure Security Agency (CISA) released an alert warning that government networks were being targeted by a spear phishing operations attributed to the Iranian state (DHS, 2019). US Cyber Command issued a warning regarding the specific vulnerability being leveraged in the operation (Vavra, 2019). The CISA statement pointed to the history of the believed perpetrators using wiper malware, hinting at data destruction as a possible aim of the ongoing operation. There were no reports of successful intrusion attempts, nor of any payload deployment and direct effects stemming from the operation. This is the first time in the timeframe studied that a US federal agency openly attributes an ongoing operation.

From August through September 2019, Iranian actors attempted to breach the email accounts of current and former US government officials, as well as people tied to the Trump presidential campaign (Perlroth and Sanger, 2019). Microsoft issued a warning of these attempts in October and attributed the activity to the Iranian-linked group Phosphorous. Microsoft registered 2,700 attempts at identifying accounts of specific people, and 241 attempts at gaining access to these accounts. Only four instances were successful, none of these were tied to official US functions or the Trump presidential campaign (Burt, 2019). This operation was rather unsophisticated and appeared to attempt to guess people's passwords based on publicly available information (Perlroth and Sanger, 2019).

Between October and November 2019, an Iranian group named APT33 or Elfin focused its year-long password spraying operation targeting about 2,000 organizations and increasing the number of accounts within these tenfold, according to Microsoft. Half of the top 25 victims were in the supply chain of industrial control systems (Greenberg, 2019; O'Flaherty, 2019). The intention of the operation is not clear, but sources at Microsoft told reporters that the group may be "laying the groundwork" for a physical attack, although no direct evidence pointed in that direction (O'Flaherty, 2019).

4.1.5 January 2020 to December 2020: Soleimani assassination - end 2020

The next peak in the relationship occurred on January 2, 2020, when General Qassem Soleimani of the IRGC's Quds Force was assassinated in a US drone strike during a visit in Iraq. Iran responded through political and militarily escalatory moves. First, President Rouhani's Cabinet declared on January 5 that Iran would conduct the fifth and final step in the gradual decrease in compliance with the JCPOA. This entailed eliminating all imposed restrictions on nuclear activities, including volume of enriched material, enrichment degree, further research on nuclear related issues and enrichment capabilities (IRNA, 2020b). On January 7, the Iranian parliament designated all US military forces as terrorists (Al Jazeera English, 2020).

Iran responded militarily to the Soleimani assassination on January 8 by firing 11 missiles at the Ain Al-Asad base in western Iraq where US and allied troops were stationed, and two missiles at a base near Erbil further north. Two missiles had unknown impact sites. The attacks caused 11 injured US troops and material damage (Baron, 2020; Dehghanpisheh, Hafezi and Aboulenin, 2020; Karimi, Vahdat and Gambrell, 2020; Martinez and McLaughlin, 2020). This incident was a clear and significant escalation of the situation. However, none of the parties seemed to wish to escalate the situation any further. The United States did not issue a response of a similar severity, which eased the fears of war. Foreign Minister Zarif said the strikes "concluded" the Iranian response, although some military leaders appeared to hint at further action. US intelligence alluded to Iran standing down (Dehghanpisheh, Hafezi and Aboulenin, 2020). Additionally, Iran had taken steps that seemed to limit the escalation hazard while portraying the attack to domestic audiences as more severe than it was. Tehran warned about the strike beforehand, giving the targets time to prepare. Iranian news media reported that the attack had caused 80 deaths among US troops, a falsity aimed at satisfying the domestic anti-American sentiment to retaliate with significant severity without provoking a response they could not sustain (Mehr News Agency, 2020).

Iran's political escalation toward the United States in January 2020 was coupled with a continuation of the post May-2018 strategy of attempting to pressure the US allies to side with Tehran and persuade the US to decrease tensions. The European parties, meanwhile, activated the Special Dispute Mechanism in the Deal on January 14, 2020 on the basis of Iran's decision to begin enriching activities at the Fordow facility (Irish and Faulconbridge, 2020). This was met with harsh criticism in Moscow and Beijing and seen as an escalation of importance form Tehran's point of view, as it entailed a formal accusation of breaching the agreement and opened for re-imposing additional sanctions. Iran's Foreign Minister Zarif warned that it would withdraw from the Non-Proliferation Treaty if asked to meet in the UN Security Council as a result of the Mechanism being enacted.

The spring of 2020 showed further cracks in the diplomatic 'high-ground' that Iran guarded since the US exit from the JCPOA. In March, the IAEA stated that their requests to gain access to certain locations had been ignored. In June, IAEA reported suspected non-disclosed facilities dating back to before 2003 (IAEA, 2020b). On June 11, the IAEA issued a list of suspected Iranian nuclear proliferation activities, which resulted in a resolution from the IAEA Board of Governors on June 19 (Davenport and Masterson, 2020a). This sparked strong discontent in Tehran, prompting the Iranian Parliament to pass a statement to halt implementation of the Additional Protocol which ensured the IAEA access to Iranian infrastructure for investigative purposes (Tehran Times, 2020). This statement was signed by 240 lawmakers but not enforced by the government. President Rouhani warned of a “stern response" to the resolution by the IAEA Board of Governors (Karimi, 2020b). On July 3, Iran triggered a dispute mechanism in the JCPOA, citing the European parties’ failed implementation. The dispute was defused in August when Iran granted the IAEA access to the sites requested (IAEA, 2020a). A September report from the IAEA stated that stockpiles continued to increase, while the Additional Protocol was still implemented (Director General IAEA, 2020).

Washington introduced sanctions on different entities throughout this period, while engaging in a diplomatic push to put pressure on Tehran. The president of Iran’s Atomic Energy Organization, Ali Akbar Salehi, was sanctioned in late January, followed by entities accused of facilitating the IRGC’s economic activity and construction companies later in the spring (Pamuk and Irish, 2020; USDS, 2020a). In late April 2020, the United States began the last diplomatic push to escalate politically toward Tehran. A clause in the 2231 resolution, prohibiting sales of arms to Iran, was set to expire in October 2020. The US presented a draft resolution in the UN Security Council in June 2020, which would re-instate the pre-2015 UN-sanctions on Tehran. The resolution was defeated, however. Washington announced in August 2020 that that it would introduce the snapback sanctions unilaterally on September 20 (USDS, 2020b). The JCPOA Joint Commission issued a statement underlining that the US was not considered a party to the Deal and that the European parties would not honor any unilateral snapback sanctions (Chair of the JCPOA Joint Commission, 2020). UN Secretary-General Guterres also issued a statement saying that he would take no steps to implement the US unilateral sanctions (Nichols, 2020). The last escalatory attempt from the US failed to create momentum in pressuring Iran. Consequently, the UN embargo on arms sales to Tehran expired on October 18. In late September and October 2020, Washington issued the last two rounds of sanctions against Iran's Ministry of Defense and the army's logistics branch, as well as banks and the oil sector, for terrorism-related activities (USDS, 2020; USDT, 2020b).

In February and April 2020, Iran attempted two satellite launches using the Simorgh and Qased launch vehicles, respectively (Fars News Agency, 2020). Only the April launch was successful in launching a satellite into orbit and marked a turning point in three ways: It was the first successful space launch since 2015, the first using Qased as a launch vehicle, and the first to be conducted by the IRGC, and not the civilian Iranian Space Agency (Hafezi and Stewart, 2020; Hinz, 2020; Wall, 2020). This is significant because up until then only the civilian Space Agency had conducted such launches. Hence, the April launch revealed a parallel military satellite program for the first time (Hinz, 2020). On June 18, 2020, Iran tested a cruise missile during a naval exercise in the Gulf (AP, 2020). Later in July, the IRGC launched ballistic missiles from an underground launch site during a military exercise near the Persian Gulf (IRNA, 2020a; Vahdat and Gambrell, 2020). This exercise was among the larger operations completed by Iran, sending a stern signal in the tense atmosphere of the summer 2020 where the last diplomatic push of the US for re-instating sanctions coincided with the tensions between Tehran and the remaining parties to the Deal.

In the fall of 2020, Iran continued the gradual political escalation seen the preceding year by expanding its nuclear activity. Several explosions and fires of unclear origin occurred on different industrial sites across Iran, including nuclear facilities of Natanz, in the summer (Gol, 2020; Radio Farda, 2020). This prompted Iran to open a new centrifuge manufacturing factory in September 2020, which replaced the lost enrichment capability (Reuters, 2020; Rising, 2020). Iran's energy minister announced that the output from the Bushehr nuclear power plant would be increased threefold, to 3 gigawatts (PressTV, 2020). Meanwhile, Iran began using advanced IR-2 centrifuges for enriching uranium gas, another breach of the JCPOA (Murphy, 2020). An IAEA report stated in

November 2020 that the stockpile of uranium enriched at 4.5% had reached 2,443 kg (Davenport and Masterson, 2020b).

A final significant political escalation took place on November 3, when the newly elected Iranian parliament dominated by hardline candidates passed a bill including several significant increases in the enriching activity and degree (Karimi, 2020a). Among the most controversial proposals related to the Fordow facility, allowing it to begin enriching uranium to 20% purity, which entailed it could become usable for producing a nuclear weapon. Additionally, the bill called on the government to decrease access for international observers and to halt the voluntary implementation of the Additional Protocol if banking relations and oil sales to Europe did not return to normal (Middle East Monitor, 2020). This political escalation was seen by some as an attempt to give Iran leverage before entering negotiations with the new US administration the following year and to pressure the remaining parties to the deal to provide relief from the sanctions.[24] President Rouhani attempted to mediate the political escalation resulting from the new legislation, deeming it harmful to negotiations. He refrained from signing it into law and stated on several occasions that every nuclear activity could be halted and reversed (Motamedi, 2020). Construction works at Fordow were revealed on December 18, although with few details available (Gambrell, 2020).

4.1.5.1 Iranian cyber operations

During this period, the intensity of cyber operations of the preceding seven months continued, with six entries in the dataset. The CISA issued warnings of feared increase in cyber operations in the wake of Soleimani's assassination (Cybersecurity and Infrastructure Security Agency, 2020b). Two operations took place in January 2020. The first was revealed by cyber security firm Dragos, identifying increased efforts by two Iran-linked groups that attempted in concert to gain access to US electric utilities and oil and gas firms through password-

[24] In contrast, some observers viewed the bill as deliberate sabotage of the JCPOA, attempting to make it more politically difficult for the Biden Administration to re-enter the Deal (Hafezi, 2020). Some factions in parliament suspected that the IAEA inspectors had been a source of intelligence in preparations for the assassination of nuclear scientist Fakhirzadeh (Karimi, 2020a).

spraying and vulnerabilities in VPN software (Dragos, Inc, 2020; Greenberg, 2020). The campaign had been active throughout 2019 but increased in intensity in early 2020. The report did not indicate whether the efforts had been successful in creating breaches but stated that the operation had not reached the industrial control systems. Toward the end of January of 2020, an operation was revealed where Westat, a US firm, had been impersonated in a spear phishing operation for infiltration efforts against several private companies and federal agencies. The group responsible was APT34 or OilRig. According to media reports, the spear phishing campaign was successful in installing two sets of malware on the target computers of an unknown number of federal systems. One created a backdoor while the other a program to intercept passwords (Cimpanu, 2020b; Litvak and Kajiloti, 2020). No information on wider implications of the operation has been disclosed.

Between May and June 2020, the Iranian group Phosphorous attempted to access the email accounts of officials in the Trump Administration and the Trump election campaign (Burt, 2020; McMillan, 2020). The attempts came in the form of a spear phishing operation but were unsuccessful, according to Microsoft (Burt, 2020). The FBI issued an alert to private industry actors in early August 2020 regarding attempts by an Iranian group exploiting recently disclosed vulnerabilities in software widely used by large private companies and government bodies. The group was disclosed by sources as Fox Kitten or Parasite, well known for the tactic of providing access for other Iranian groups to exploit (Cimpanu, 2020a). The campaign focused on a particular vulnerability in a popular product 'BIG-IP' of the US company F5 Networks. The product is widely used by large corporations and government agencies. Only two instances of successful breaches were reported, both on private companies (Cimpanu, 2020a).

In September 2020, the CISA issued an alert of Iranian hacker activity targeting a wide cross section of federal government, telecommunication, IT, healthcare and financial entities through exploiting vulnerabilities in VPN software (Cybersecurity and Infrastructure Security Agency, 2020a). The CISA alert pointed out that the actor appeared to be focusing on maintaining a foothold in the systems and exfiltration of data, and was known to have sold access on hacker forums for financial gain. The actor was viewed by CISA as a contractor of the Iranian government. FBI concluded that the actor had the capability and likely intent to unleash ransomware in the systems breached (Cybersecurity and Infrastructure Security Agency, 2020a).

In October 2020, CISA and the FBI revealed that Iranian groups had probed an unknown number of websites connected to the election process in 10 US states. The operation used open-source tools and appeared to be looking for obtaining voter data (Lyngaas, 2020a). In one instance, the groups were successful. This operation emerged in the context of a wider voter intimidation campaign attributed to Iran, which appeared to have been the end goal of the probing operations. Although not part of the cyber operations studied in this study, the voter intimidation efforts are crucial as they shaped the context within which the operation in October took place, and colored the perception of the severity of the operation. In the week prior to the revelations, a wave of illicit emails impersonating the militant group Proud Boys,[25] containing threatening content urging the recipient to vote for the incumbent presidential candidate, were issued to some Democratic voters in Florida, a key swing state in the 2020 presidential election (Owen and Francheschi-Bicchieria, 2020). The voter intimidation effort was swiftly attributed to Iran by the Director of National Intelligence and Director of the FBI (Vavra and Lyngaas, 2020). The day following the attribution, the Treasury Department issued sanctions on several Iranian entities, including the IRGC, for election interference through influence operations (Lyngaas, 2020b; USDT, 2020a). Both events appeared to have been conducted by using data openly available. Although the operation was only successful in obtaining access to *one* voter registration database, the wider impression of vulnerability of foreign influence on the US democratic process remained.

[25] The Proud Boys are a violent white supremacist militia group that were vocal supporters of President Trump, and especially visible in the run-up to the 2020 presidential election (Wendling, 2020).

4.2 The role and utility of cyber operations

This second level of analysis will first conclude the hypothesis test conducted by the preceding analysis and confirm the validity of the two expectations based on the data and literature underpinning this study. It will continue to outline the conditions under which cyber operations were used and examine the role of cyber operations in Iranian policy from the pattern described in the preceding sub-chapter. At its close, a discussion on the utility of the operations will follow, expanding on how the cyber operations can be seen as advancing Iran's position in the feud through increasing the power of the Islamic Republic or degrading the US sources of power.

4.2.1 Result of empirical test

The preceding analysis has tested the hypothesis "the cyber operations will follow the escalation dynamic in the other domains". Its results are affirmative. The use of cyber operations broadly followed the escalation dynamic in the context and in the conventional policy domains of the Islamic Republic. In the three major escalation milestones presented – the US exit from the JCPOA, Iran's announcement of its decreasing compliance with the JCPOA, and finally the assassination of General Soleimani – the analysis showed that Iran remained restrained until the United States formally exited the Nuclear Deal and increased the targeting of its operations after May 2019. The intensity between May 2019 and the assassination of Qassem Soleimani in January 2020 continued after this date. The operations continued at a similar intensity throughout 2020, although one qualitative change occurred in the fall of 2020.

When approaching the dynamic escalation at a more granular level, the pattern of cyber operations does not consistently overlap with the escalatory moves by the United States or the development in the context. Only three of the 15 operations studied seemed tied to a specific event by virtue of their timing or target. The targeting of US officials charged with re-instating sanctions on the Islamic Republic in the early fall of 2018 coincided with a significant wave of sanctions. The June 2019 probing operations of government systems began quickly after the

Iranian downing of the US drone and Washington's cyber operation retaliation. Exceptionally, the operation in the fall of 2015 targeting US officials appeared to be tied to the opening of the Iranian economy resulting from the JCPOA. This example suggests the presence of conflicting interests of power centers within Iran and that cyber operations in some circumstances do not act in tandem with a governing state's policy.

Nine out of the 15 operations studied in this project were not successful in gaining access to their targets. Out of the six that were successful, only three were successful in breaching structures connected to US government structures or US officials. One of these operations produced an observable outcome, namely the voter intimidation campaign in the run-up to the 2020 presidential election. Similar to the Russian meddling in the 2016 presidential election, this operation proved to contribute to a perception of the US democratic process being compromised. As far as the available data shows, none of the operations against critical infrastructure or industrial control systems appeared to be successful. In the instances where the operations were successful in breaching private companies, no information on the wider implications was unveiled.

None of the operations studied had degradation as an outcome, confirming the expectation of the operations being non-coercive defined from the outset of this study. Four of the operations were openly attributed to the Iranian state during their activity. The voter intimidation campaign in October 2020 was among them and, issued direct response in the form of sanctions on Iranian bodies. None of these direct reactions were of significant magnitude to be considered escalatory in the sense defined by this study when "at least one of the parties involved believes there has been a significant qualitative change in the conflict as a result of the new development" (Morgan *et al.*, 2008, p. 8). The Iranian political escalations in November and December 2020 were tied to the new hardline parliament's strategy regarding the future of the JCPOA, and they were not direct responses to the new sanctions. The expectation of Iranian cyber operations not being escalatory is therefore also empirically confirmed by this study.

This study set out to assess what the qualitative or quantitative alterations in operations revealed about the role of cyber operations in Iranian policy. The quantitative alterations have been expanded on earlier in this chapter. From the US exit of the JCPOA until the summer of 2020, the targets of Iranian cyber operations had been primarily critical infrastructure, private companies in the supply chain of critical infrastructure, public agencies and individuals connected to the Trump administration or election campaign. Prior to the US exit, the targets were individuals in the State Department and one military contractor. These targets fall neatly within classical targets for espionage, subversion and potentially preparatory moves for a disruptive degradation attack. There was no *systematic* alteration in the type of targets that would indicate a conscious strategy akin to that revealed by the quantitative alteration.

However, the study found one qualitative alteration of note when Iran targeted the election infrastructure in several US states in October 2020. After completing its fifth and final step of decreasing compliance with the JCPOA in January 2020, Iran had few political tools left that it could leverage against the US or the remaining parties to the Deal. Iran continued to enrich uranium throughout 2020 and did not escalate noticeably politically in regard to the nuclear program until November 2020. The cyber operation prior to the US election in November may have altered the trend of activity in the cyber domain aimed at either increasing pressure on the US slightly more through harming or giving an impression of interference with the democratic process. This qualitative change may also simply reflect the timing, with Tehran merely taking advantage of an opportunity created by the election. Overall, the quantitative alterations revealed the most about Iran's role in the cyber operations, while the qualitative alterations contribute less to the topic studied.

4.2.2 Conditions under which cyber operations were used

The empirical analysis brought some insight into the conditions under which Iran appeared to opt for using cyber operations. The entries displayed a visible restraint when Iran had achieved its top strategic goal, between 2015 and May

2018. When the sanctions were gradually re-introduced by the United States from May 2018, Iran began deploying cyber operations again, which intensified from May 2019 when Iran began rolling back its compliance to the Nuclear Deal. This indicates that Tehran began deploying cyber operations when its top strategic aim was being *actively* challenged.

However, three points emerge in this broad pattern. Firstly, several alterations in the Iran policy of the United States after President Trump took office challenged Iran's top strategic aim. With new sanctions legislation passed, the new strategy on Iran was unveiled in October 2017 and the trust in the credibility of the JCPOA eroded gradually from its outset. Tehran continued its relative restraint in cyber space in this period, assessing whether the signs were a clear shift in tone in Washington. This restraint testifies to the consciousness of the signaling effect of cyber operations, despite their secret nature. It is likely that the diplomatic 'high ground' held by Tehran in this period played a role and that it wished to appear as *playing by the rules*. Following May 2018, amid the US exit from the JCPOA, Tehran re-iterated Washington's disregard for international law and lack of credibility in diplomatic affairs. It is in line with this strategy that Tehran tried to appear respectful of international law and norms as long as it felt that these played a part in safeguarding its primary goal.

Secondly, between May 2018 and May 2019, Iran was relatively restrained in the political domain, yet began activity in the cyber domain. This indicates that Iran chose to escalate marginally horizontally through cyber operations, while remaining politically restrained. Iran took steps politically to threaten escalation in this period, but none were in breach of the JCPOA, and the sum was restrained compared to the escalation conducted by the United States by exiting the Deal. This may indicate that choosing cyber operations *over* political or military moves made discontent visible during this time.

The third and final point regards Iranian activity after the third peak in escalations in 2020. After the assassination of general Soleimani, cyber operations conducted by Iran appeared to continue in a similar form and intensity as in the preceding seven months. Prior to the assassination, Iran had few possible means of political escalation left after having capitalized on the decreased compliance to the JCPOA through five steps. In order to express visible discontent, one could assume that Iran would favor an increase in use of cyber operations. This did not happen. This is noteworthy because it suggests a threshold of what Iran was willing to do in this domain. In half of the operations that occurred in this period, US authorities openly attributed the operations to Tehran. This only happened on one occasion before in the timespan studied. From the data available in this study, the operations in 2020 did not appear to be of either higher severity or degree of success than the preceding operations. This author suggests that this may indicate an attempt on the part of the United States to deter an eventual escalation from Tehran using cyber operations.

4.2.3 Cyber operations vis-à-vis conventional policy tools

This study set out to determine the role of cyber operations in Iranian policy towards the United States seen vis-à-vis the use of conventional foreign policy tools. Overall, the cyber operations appeared to follow the escalatory patterns in the political domain and not in the military domain. This is made visible on three points in the dynamic. Firstly, the low activity in the cyber domain between July 2015 and May 2018, when Iranian political escalation was absent but ballistic missile tests were conducted at a steady pace. Secondly, in the emergence of the cyber operations after the US exit, when Iran escalated marginally within the legal boundaries of the JCPOA. And thirdly, in the increase of intensity in the cyber domain after May 2019, when Iran began its steady political escalation through decreasing compliance with the Nuclear Deal. It is worth noting, however, that between the US exit and Iran's decrease in compliance with the Deal, Iran was more active in the cyber domain than in the political domain, where it remained overall restrained. The pattern of behavior in the political domain and in the cyber operations coincides to a larger degree compared to the military moves, although at a granular level the dynamic in the political and cyber domains do not overlap perfectly.

The pattern of behavior suggests that Iran used the political escalation moves in an attempted coercive manner. Iran was explicitly threatening escalatory steps in regard to the nuclear program following May 2018 when the situation moved in the opposite direction of their desired aim. The coercive strategy appears to have had a dual target: the United States *and* the remaining parties to the Nuclear Deal, particularly the European parties. Iran's diplomatic strategy attempted to coax the parties to make more efforts to compensate the economic implications for Tehran and to direct their diplomatic pressures toward Washington to save the JCPOA.

Meanwhile, the military moves seem to operate more independently of the diplomatic efforts to save the Deal. The ballistic missile tests and satellite launches appear to be deployed in a cyclical manner and not directly connected to the development of the context. A small decrease in military tests when the tensions between the US and Iran escalated, mainly in the two last context blocks studied, suggests there were some exceptions. One satellite launch is an outlier in this pattern. The successful April 2020 satellite launch, conducted by the IRGC and not the civilian Iranian Space Agency, communicated a *military* capability with dual use value as a ballistic missile with significant reach. This launch casts doubt on Tehran's claim that it was not developing technologies for intercontinental ballistic missiles capable of carrying a nuclear warhead.

The evidence of kinetic military engagements were stern and unambiguous escalations or retaliations of escalatory moves in the three instances in June and September 2019 and in January 2020. However, the pattern of cyber operations did not reveal a visible qualitative or quantitative alteration in close temporal proximity to the kinetic military engagements. The only exception to this pattern can be seen in two cyber operations in January 2020. Yet both operations had an activity frame that preceded the military retaliation to the Soleimani assassination.

Overall, a clear lack of correlation between military and cyber activities suggests is that cyber operations appear to be given a role of additive measures of signaling tied to the moves in the political domain. The military moves, by comparison, are dual in aim and appear to follow a parallel rationale, namely the underlining the freedom of the ballistic missile and space programs from the provisions of the Nuclear Deal, and the kinetic engagements directly tied to peaks in escalations from the adversary.

4.2.4 The role and utility of cyber operations

This study set out to determine the role and utility of the cyber operations for Iran. The only operation in the dataset that succeeded in creating *observable* outcomes was the targeting of state election sites in October 2020. The operation contributed to undermining the trust in the security of the democratic process, a key component of the identity of the United States. The US was not foreign to adversaries attempting to influence voter behavior ahead of elections. Still, the operation could be seen as an attempt to destabilize the sources of national power of the United States. While the actual impact appears to be marginal since the campaign was revealed, attributed and openly sanctioned by US authorities, the *perceived* insecurity had a positive impact on Iran's relative stance in the feud by virtue of subverting a core value of the US.

The data set shows that cyber operations had indirect and *communicative* effects that may have benefited Iran. When Iran increased its cyber operations from May 2018 and further intensified them from May 2019, it engaged in a horizontal escalation of low severity that increased their own power marginally by making visible their resistance to the developments and the continued campaign of the United States. As such, the resistance was directed toward the United States, but also its own population, hence solidifying an image of fighting tooth and nail for its citizens. This can be seen as bolstering the Iranian state's power and legitimacy as the protector from perceived unjust aggressions from outside powers. The image of Iran as a recurrent victim of aggression of foreign powers is deeply rooted in the national narrative. This stems from the long lines of Iranian history traversing empires and dynasties, but also specifically to the Shia identity of the Islamic Republic, which has been a minority branch of Islam of the oppressed.[26]

[26] See Tabatabai (2020) for a comprehensive overview of Iranian perceptions of national security.

The Islamic Republic has capitalized on this history and has engulfed it in its ideological footing. As earlier defined in chapter 3 of this study, a key motivation for relieving the sanctions is the regime security component. Making resistance visible through low-severity cyber operations is therefore an effective and low-risk way of increasing the security of the regime.

The horizontal escalation of increasing the cyber operations from May 2018 and intensifying them from May 2019 can be seen as destabilizing the US sources of power by exposing a vulnerability to intrusions by a foreign actor. The targeting of the Trump administration and the President's electoral campaign, as well as the government bodies and federal systems, could promote a *perceived* vulnerability in the United States. The operations do not need to be successful in order to have the effect of revealing a*n ability* to touch or target structures of value. The secrecy surrounding cyber operations can spark fears of the outcome being more severe than in reality. The targeting of critical infrastructure plays along the same lines. Three of the Iranian operations were targeting critical infrastructure such as electric grids and companies in the supply chain of industrial control systems. One operation was part of a wider global campaign, while and two others more directly targeting the United States. The mere attempt to breach said systems can have a desired effect of communicating vigor in the intruder and vulnerability of the target. The incapacitation of critical infrastructure is a widely used alarmist scenario of the destructive potential of cyber operations. Targeting entities in this sector exploits this fear and plays to the portrayal of Iranian efforts nearing dangerous outcomes.

This author derives from the empirical analysis that the low-severity cyber operations for Iran function as a low-risk communicative tool that can nourish an image of persistence to the United States and the Iranian population, without a significant risk of escalating the relationship out of the agreed battle into a kinetic confrontation. Cyber operations function as ambiguous signaling tools and can be read differently by different audiences. In the wake of the diplomatic failures to save the Nuclear Deal, the Iranian regime may have sensed a need to signal resistance, both to the US and its own population, with low-severity cyber operations as a compelling option. Assuming that US media outlets would report on such matters, Iran could be certain that its resistance through cyber operations, however qualitatively insignificant they were, could be *perceived* as a response of importance. The psychological aspect of cyber operations may therefore constitute a large part of their effectiveness for Iran.

Chapter 5 – Discussion of findings and conclusion

This study set out to answer the research question "what is the role of cyber operations in Iran's policy toward the United States." This study concludes that the role of cyber operations in Iranian policy toward the United States is as a communicative tool signaling broad political stances. This was evidenced by the relative tranquility in the cyber domain from 2015 until May 2018 and the emergence of activity from this point onward. The restraint implies that Tehran was conscious of the signaling effect of the activity and refrained from deploying cyber operations in this period. Had this not been the case, Tehran may have deployed a steady number of cyber operations regardless of the development in the context. The relative tranquility in the first three years further evidences that Tehran do not consider the cyber operations truly *covert.*

The pattern of the cyber operations studied indicates that the operations do not appear to be rigorous tools of either pressure or communication, although a few instances of cyber operations act as direct responses to specific events. It is evidenced through the affirmation of the hypothesis that the cyber operations do broadly follow the escalation in other domains. However, at a more granular level the activity does not overlap the escalatory moves by the United States, nor the political or military pattern of activity of Iran. The pattern of activity of cyber operations corresponded to a larger degree with the political moves by the Islamic

Republic than to the policy of military nature. This indicates that the operations have a role of additive signaling to the political moves.

From the outset of this study, three expectations to the object of study were presented. Two from the literature on state-sponsored cyber operations and one derived from logic. These suggested that cyber operations deployed by Iran would be non-coercive in nature, and not escalatory, while they would advance Iran's stance in the feud in some way. All these expectations were confirmed by the empirical analysis. In this respect, this study has evidenced that cyber operations of low severity can have a positive effect on a state's contemporary policy within a dynamic feud, that coercion is not the only outcome of strategic value from activity in cyber space, and finally that this can be obtained without notable risk of unwanted escalation.

5.1 Implications for the academic field and policy

The findings of this study have implications for several branches of the literature. Firstly, they offer some moderate support to the branch of literature on strategy and cyberspace that holds that states can advance strategic goals short of war in the fifth domain (Fischerkeller and Harknett, 2019b; Harknett and Smeets, 2020). Strategic effects are defined differently in the literature treated in this study, focusing mainly on *material* underpinnings of national power and the relative placing of states in the international system (Fischerkeller and Harknett, 2019b; Harknett and Smeets, 2020). The *strategic* component of the findings of *this* study was overall more indirect in nature through strategic signaling, and only on one occasion with observable outcomes.

Secondly, the findings of this study support the view that the entrance of cyber operation in the dynamic of a feud does not have to increase the risk of significant escalations in other domains (Gartzke and Lindsay, 2015; Borghard and Lonergan, 2019; Fischerkeller and Harknett, 2019a; Jensen and Valeriano, 2019). The reasons for this not being the case are portrayed differently by various scholars. What *this* study shows is that the conscious use of cyber operations did not create escalations, and yet had a positive indirect impact on the stance of the object of study. The positive impact also occurred without the cyber operations being coercive, understood in this study as having degradation as an outcome (Valeriano et al 2018, pp.78-83). Further, these findings indicate that even when Iran had a top strategic aim challenged, it did not attempt to coerce or escalate the feud through cyber operations. Yet it *ameliorated* its own position marginally through the use of cyber operations.

The character of cyber operations as 'open secrets' that carry signaling value is supported by the empirical analysis of this study. As pointed to in chapter 2 of this study, some authors hold that state activities that are exercised covertly hold no conscious signal because they are not intended to be revealed (Borghard, 2018). Had this been the case for Iran, one could argue that the relative restraint seen between July 2015 and May 2018 would not have taken place. This indicates that Tehran is conscious of its operations' possible impact on the mutual de-escalation in the period when the JCPOA was being gradually implemented and Iran's strategic aim was obtained. This would provide empirical validity to the understanding of the branch of the literature that claims that covert statecraft do carry signaling value (Carson and Yarhi-Milo, 2017; Cormac and Aldrich, 2018; Valeriano, Jensen and Maness, 2018). However, the relative restraint from 2015 until May 2018 directly contradicts one claim made in the literature cited in this study. Brantly (2016, p. 18) stated that hostile covert action, to which he placed cyber operations, did not demand an open sacrifice of political capital. The results of this study contradict this statement. Had cyber operations not entailed any political cost for Tehran, it would have few incentives to hold on to relative restraint when the situation was in Tehran's favor.

This study has illustrated how the ambiguity of the signaling power of cyber operations is a double-edged sword. On the one hand, threat inflation of cyber operations may cause undue fear. But they can also create an option for retaliation or policy that is relatively harmless, and be *perceived* as a sterner response by the general public than it is (Libicki and Tkacheva, 2020). In cases like Iran's, whose legitimacy is based on resistance to external powers, this can be useful and decreases the escalation risk in the feud. In this respect, the result of this study supports the branch of scholarship that views the usefulness of cyber operations as an escalatory offramp stabilizing the feud, as it offers a less severe policy option to impose signaling compared to other means available (Jensen, 2017; Jensen and Valeriano, 2019). The findings also support the conclusion of Valeriano et al. (2018, p.88) that low-severity cyber operations between adversaries are more of a stabilizing dynamic that aids the parties in *avoiding* escalations in other domains than an effective coercive tool. The same authors have deemed cyber operations as 'additive measures' that amplify existing signals (Valeriano, Jensen and Maness, 2018, p. 23). This study supports this claim, evidenced by the broadly corresponding pattern of behavior between the political moves and the cyber operations.

The findings of this study strengthen the scholarship on policy in cyberspace that holds that cyber operations of low-severity can have a positive effect on state's stance in an adversarial relationship. Although the *direct* effects of the operations were almost absent, the indirect and communicative effects were positive for Tehran. This study indicates that the entrance of cyber operations in a dynamic feud does not have to increase the escalation risk in the relationship if the wielder of the operations can obtain a needed effect through low-severity operations. Thus, the presence of cyber operations is seen as stabilizing as an alternative option for signaling discontent with low escalatory risk.

5.2 Limitations and suggestions for further research

There are limitations to this study that affect the level of confidence in the different findings from the empirical analysis and the conclusions drawn. Firstly, the covert nature of cyber operations opens for the possibility that the dataset does not reflect the actual activity. Often, cyber operations are revealed some time after they have been conducted. The temporal window studied until the end of 2020 increases the chances of some cyber operations are yet to revealed. However, the expectations of the operations being non-coercive and non-escalatory would likely remain affirmative. A coercive or escalatory cyber operation would likely have been observable in the dynamic of the relationship. Also, the key finding of this study was the presence of the relative restraint between 2015 and May 2018, and the emergence of activity after this point. These findings are less likely to be altered by new revelations of cyber operations because of the time passed.

The level of detail available on the *exact* parameters of the operations, their targets, timing of emergence and actual implications were not available in the majority of the entry points in the dataset. This lack of precise information made it difficult to establish with certainty the level of precision of the cyber operations seen in relation to the development on the feud. This decreases the level of confidence in this specific conclusion. Considering how detailed information about cyber operations tend to emerge as time passes, it would be beneficial to re-visit the dynamic studied in this research project at a later stage to account for the eventual presence of other operations with features that counter this author's escalation hypothesis.

This study treated the Iranian state as a single actor and did overall not consider the conflicting interests and power centers within the state. The political system of the Islamic Republic is a mixture of elected and appointed bodies, and of civil and religious authority. A complex governing structure is overlapped by opaque power structures and widespread corruption. The military structure is split and arranged under different authorities in the governing structure. On top of this come the Iranian proxy actors, which are also active in cyberspace (Maurer, 2018, chap. 5). This complex system suggests a possible disconnect between the deployment of cyber operations and the remaining policy at large. This decreases somewhat the level of confidence in the *conscious* aspect of the deploying cyber operations at specific times. Including such aspects in further research on Iranian cyber operations is recommended.

Iran's top strategic goal and the core of the feud with the United States has been defined as relieving the sanctions pressure. As shown in chapter 4, Tehran attempted to pressure the remaining parties to the JCPOA on several occasions to invest more political capital in pressuring the United States and salvage the

Nuclear Deal. Examining the pattern of Iranian cyber operations targeting the other diplomatic parties with influence on the fate of the JCPOA may have helped advance the understanding of the utility of cyber operations as tools for obtaining the top strategic goal.

This study has only examined two groups of conventional policy tools. Future examination of case studies where states have wider arsenal of conventional policy tools at their disposal should increase the understanding of the place of cyber operations vis-à-vis conventional tools. Such studies would benefit from both granular examinations over short time periods and larger studies spanning across years. Approaches examining synergies between the use of cyber operations and other tools of policy would greatly benefit the field. There are indeed some approaches considering this field of study (Reichborn-Kjennerud and Cullen, 2016; Cullen and Reichborn-Kjennerud, 2017). However, these approaches are focusing on the place of cyber operations in armed conflict and not in the strategic space discussed in this study. Examining how cyber operations may work as additive measures to other tools of policy than the ones treated in this study, as well as how such measures obtain other types of strategic aims, may also bring more value to the field.

The assumption underpinning this study of the cyber operations being non-coercive in nature was confirmed by the empirical analysis. However, the definition of what constituted a *coercive* operation (degradation as an outcome) was building on an understanding of coercion closely tied with classical approaches to force and punishment. Other scholarship is seeking to re-define what a coercive strategy in cyberspace would entail and explore new understandings of coercion that distance themselves from how coercion looks in conventional domains. Jensen (2017) is one example that views the coercive effect of cyber operations as the additive measures evidenced through this study. This study has showed that low-severity cyber operations *can* be of use for states in a dynamic feud. Future scholarship may examine further how to conceptually re-define the abilities of states in this domain.

A key entry point for this study was to examine when a state *chooses* cyber operations to advance its interests. The case of Iran was selected on the basis of an assumption that the state would chose to remain within the strategic space short of war. However, the low severity of operations examined in the study may result from the lack of *ability*, not of *will*. As put forward in chapter 2 of this study, a cyber intrusion can communicate a wider array of messages (Borghard, 2019). An attempt to penetrate critical system may then be an explicit threat and display of heart-felt will to disrupt or degrade key functions of a state's public or private infrastructure. Without intimate knowledge of the inner workings of the Iranian offensive cyber power apparatus, open sources will always come short of the clear-cut answers.

This chapter has pointed to some contributions of this study and some recommendations for further research. However, much work remains for conceptually grasping the implications of the emergence of the fifth domain on international relations. We are still only observing the first waves of approaches to making use of the cyber domain for advancing policy, and much remains to be revealed about the impact and wider ramifications of this field.

References

Abdollah, T. (2019) *AP sources: US struck Iranian military computers this week*, *AP NEWS*. Available at: https://apnews.com/article/iran-nuclear-politics-donald-trump-iran-international-news-f01492c3dbd14856bce41d776248921f (Accessed: 20 April 2021).

Al Jazeera (2017) *US hits Iran with fresh sanctions over space launch*, *Al Jaseera English*. Available at: https://www.aljazeera.com/news/2017/7/28/us-hits-iran-with-fresh-sanctions-over-space-launch (Accessed: 16 June 2021).

Al Jazeera (2019a) *Iran unveils cruise missile on revolution anniversary*, *Al Jazeera*. Available at: https://www.aljazeera.com/news/2019/2/2/iran-unveils-new-cruise-missile-on-islamic-revolution-anniversary (Accessed: 17 June 2021).

Al Jazeera (2019b) *Iran's Rouhani announces another step away from 2015 nuclear deal*, *Al Jazeera*. Available at: https://www.aljazeera.com/news/2019/11/5/irans-rouhani-announces-another-step-away-from-2015-nuclear-deal (Accessed: 28 April 2021).

Al Jazeera English (2020) *Iran's parliament designates all US forces as 'terrorists' | Soleimani assassination News | Al Jazeera*, *Al Jazeera*. Available at: https://www.aljazeera.com/news/2020/1/7/irans-parliament-designates-all-us-forces-as-terrorists (Accessed: 27 April 2021).

Ali, I. and Stewart, P. (2019) 'Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials', *Reuters*, 16 October. Available at: https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK (Accessed: 26 April 2021).

Allison, G. T. and Zelikow, P. (1999) *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd edn. Pearson.

Anderson, C. and Sadjadpour, K. (2018) *Iran's Cyber Threat: Espionage, Sabotage and Revenge*. Carnegie Endowment for International Peace, p. 86. Available at: https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf (Accessed: 19 April 2021).

Anderson, E. E. (1998) 'The security dilemma and covert action: The Truman years', *International Journal of Intelligence and CounterIntelligence*, 11(4), pp. 403–427. doi: 10.1080/08850609808435385.

Annan, N. (2018) 'Pompeo adds human rights to twelve demands for Iran', *Iran Source*, 23 October. Available at: https://www.atlanticcouncil.org/blogs/iransource/pompeo-adds-human-rights-to-twelve-demands-for-iran/ (Accessed: 1 July 2021).

Associated Press (2019) *The Latest: Iran responds to US, labels CENTCOM terrorist*, *AP NEWS*. Available at: https://apnews.com/article/north-america-donald-trump-ap-top-news-terrorism-international-news-f635668cc3d6478984ddcb39dd7c78c8 (Accessed: 27 April 2021).

Associated Press (2020) *Iran test fires cruise missiles resistant to 'electronic war,' says naval chief*, *Defense News*. Available at: https://www.defensenews.com/training-sim/2020/06/18/iran-test-fires-cruise-missiles-resistant-to-electronic-war-says-naval-chief/ (Accessed: 17 June 2021).

Axe, D. (2019) *Why the Royal Navy Is Carefully Escorting Its Ships That Pass near Iran*, *The National Interest*. The Center for the National Interest. Available at: https://nationalinterest.org/blog/buzz/why-royal-navy-carefully-escorting-its-ships-pass-near-iran-79126 (Accessed: 23 July 2021).

Axworthy, M. (2016) *Revolutionary Iran: a history of the Islamic republic*.

Azer News (2019) *Iranian president announces installation of IR-9 centrifuge soon*, *AzerNews.az*. Available at: https://www.azernews.az/region/157272.html (Accessed: 28 April 2021).

Aziz, A. (2018) 'Here's How Protests and Strikes Are Leading Change in Iran', *Iran Source*, 20 December. Available at: https://www.atlanticcouncil.org/blogs/iransource/here-s-how-protests-and-strikes-are-leading-change-in-iran/ (Accessed: 7 July 2021).

Baezner, M. (2019) *Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions*. Zurich: Center for Security Studies (CSS), ETH Zürich, p. 36. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf (Accessed: 19 April 2021).

Barnes, J. E. and Gibbons-Neff, T. (2019) 'U.S. Carried Out Cyberattacks on Iran', *The New York Times*, 22 June. Available at: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html (Accessed: 19 April 2021).

Baron, K. (2020) *Eleven US Troops Were Injured in Jan. 8 Iran Missile Strike*, *Defense One*. Available at: https://www.defenseone.com/threats/2020/01/eleven-us-troops-were-injured-jan-8-iran-missile-strike/162502/ (Accessed: 17 June 2021).

BBC (2016) 'Iran: US imposes new sanctions over missile test', *BBC News*, 17 January. Available at: https://www.bbc.com/news/world-us-canada-35338901 (Accessed: 16 June 2021).

BBC News (2018a) 'International Court of Justice orders US to ease Iran sanctions', *BBC News*, 3 October. Available at:

https://www.bbc.com/news/world-middle-east-45729397 (Accessed: 27 April 2021).

BBC News (2018b) ‘Trump and Macron hint at new Iran nuclear deal’, *BBC News*, 25 April. Available at: https://www.bbc.com/news/world-us-canada-43887061 (Accessed: 26 July 2021).

Borghard, E. D. (2018) ‘The “Known Unknowns” of Russian Cyber Signaling’, *Council on Foreign Relations*, 2 April. Available at: https://www.cfr.org/blog/known-unknowns-russian-cyber-signaling (Accessed: 24 May 2021).

Borghard, E. D. and Lonergan, S. W. (2019) ‘Cyber Operations as Imperfect Tools of Escalation’, *Strategic Studies Quarterly*, 13(3), pp. 122–145.

Brantly, A. F. (2016) *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens, GA, UNITED STATES: University of Georgia Press. Available at: http://ebookcentral.proquest.com/lib/gla/detail.action?docID=4471218 (Accessed: 19 May 2021).

Brumfiel, G. (2019) *Iranian Rocket Launch Ends In Failure, Imagery Shows*, *NPR.org*. Available at: https://www.npr.org/2019/08/29/755406765/iranian-rocket-launch-ends-in-failure-images-show (Accessed: 17 June 2021).

Burns, R. and Reichmann, D. (2019) *US officials: Iran test-launched a medium-range missile*, *AP News*. Available at: https://apnews.com/article/economy-hogan-gidley-donald-trump-ap-top-news-persian-gulf-tensions-eb3ffe2c36c54a69b3ed6946f334e3b8 (Accessed: 17 June 2021).

Burt, T. (2019) ‘Recent cyberattacks require us all to be vigilant’, *Microsoft On the Issues*, 4 October. Available at: https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/ (Accessed: 16 April 2021).

Burt, T. (2020) ‘New cyberattacks targeting U.S. elections’, *Microsoft On the Issues*, 10 September. Available at: https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/ (Accessed: 16 April 2021).

Byman, D. and Waxman, M. C. (2002) *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. New York: Cambridge Univ. Press (RAND studies in policy analysis). Available at: https://www.rand.org/pubs/commercial_books/CB400.html.

Carson, A. M. (2018) *Secret wars: covert conflict in international politics*. Princeton, NJ Oxford: Princeton University Press (Princeton studies in international history and politics).

Carson, A. and Yarhi-Milo, K. (2017) 'Covert Communication: The Intelligibility and Credibility of Signaling in Secret', *Security Studies*, 26(1), pp. 124–156. doi: 10.1080/09636412.2017.1243921.

Cavaiola, L. J., Gompert, D. C. and Libicki, M. (2015) 'Cyber House Rules: On War, Retaliation and Escalation', *Survival: Global Politics and Strategy*, 57(1), pp. 81–104. doi: 10.1080/00396338.2015.1008300.

Cavelty, M. D. (2008) 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', *Journal of Information Technology & Politics*, 4(1), pp. 19–36. doi: 10.1300/J516v04n01_03.

Center for Strategic and International Studies (2021) *CSIS Database of Significant Cyber Incidents sinde 2006*, *Center for Strategic and International Studies*. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210326_Significant_Cyber_Events.pdf?ZKJIdGVXdQd2vXW.gFEcFQs2Ay7cDiqt (Accessed: 9 April 2021).

Certfa Lab (2018) 'The Return of The Charming Kitten - Certfa Lab', *Certfa*, 13 December. Available at: https://blog.certfa.com/posts/the-return-of-the-charming-kitten/ (Accessed: 1 July 2021).

Chabba, S. (2017) *Iran Preparing For War? Hormuz-2 Ballistic Missile Successfully Test-Fired*. Available at: https://www.ibtimes.com/iran-preparing-war-hormuz-2-ballistic-missile-successfully-test-fired-2505932 (Accessed: 16 June 2021).

Chair of the JCPOA Joint Commission (2020) *Chair's Statement following the 1 September meeting of the Joint Commission of the Joint Comprehensive Plan of Action*, *EEAS - European External Action Service - European Commission*. Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/84643/chairs-statement-following-1-september-meeting-joint-commission-joint-comprehensive-plan_en (Accessed: 14 June 2021).

Charbonneau, L. (2015) 'Iran's October missile test violated U.N. ban: expert panel', *Reuters*, 15 December. Available at: https://www.reuters.com/article/us-iran-missiles-un-exclusive-idUSKBN0TY1T920151215 (Accessed: 16 June 2021).

Charbonneau, L. and Nichols, M. (2015) 'U.S. conducting "serious review" of alleged Iran missile test', *Reuters*, 8 December. Available at: https://www.reuters.com/article/us-iran-missiles-usa-idUSKBN0TR2G920151208 (Accessed: 16 June 2021).

Chesney, R. and Smeets, M. (2020) 'Policy Roundtable: Cyber Conflict as an Intelligence Contest', in *Texas National Security Review*. *Cyber Conflict as an Intelligence Contest*, Texas National Security Review. Available at:

http://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/ (Accessed: 3 October 2020).

Cimpanu, C. (2020a) *FBI says an Iranian hacking group is attacking F5 networking devices*, *ZDNet*. Available at: https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/ (Accessed: 9 April 2021).

Cimpanu, C. (2020b) *Iranian hackers target US government workers in new campaign*, *ZDNet*. Available at: https://www.zdnet.com/article/iranian-hackers-target-us-government-workers-in-new-campaign/ (Accessed: 21 April 2021).

Clapper, J. R., Lettre, M. and Rogers, M. S. (2017) *Joint Statement for the Record to the Senate Armed Services Committee, Foreign Cyber Threats to the United States*. Washington, D.C., USA. Available at: https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf (Accessed: 23 May 2021).

Clark, S. (2019) 'Second Iranian satellite launch attempt in a month fails – Spaceflight Now', *Space Flight Now*, 11 February. Available at: https://spaceflightnow.com/2019/02/11/second-iranian-satellite-launch-attempt-in-a-month-fails/ (Accessed: 17 June 2021).

Corker, B. (2017) *S.722 - 115th Congress (2017-2018): Countering Iran's Destabilizing Activities Act of 2017*. Available at: https://www.congress.gov/bill/115th-congress/senate-bill/722 (Accessed: 26 April 2021).

Cormac, R. and Aldrich, R. J. (2018) 'Grey is the new black: covert action and implausible deniability', *International Affairs*, 94(3), pp. 477–494. doi: 10.1093/ia/iiy067.

Council of Foreign Affairs (2021) *Tracking State-Sponsored Cyberattacks Around the World*, *Council on Foreign Relations*. Available at: https://www.cfr.org/cyber-operations (Accessed: 30 July 2021).

Cullen, P. and Reichborn-Kjennerud, E. (2017) *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, p. 36.

Cybersecurity and Infrastructure Security Agency (2020a) *Iran-Based Threat Actor Exploits VPN Vulnerabilities | CISA*, *Cisa.gov*. Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-259a (Accessed: 9 April 2021).

Cybersecurity and Infrastructure Security Agency (2020b) 'Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad', *National Cyber Awareness System - Alert*, 6 January. Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-006a (Accessed: 4 July 2021).

Dadouch, S. (2019) 'Iranian president backs French plan to restart talks with the U.S.', *Washington Post*, 2 October. Available at: https://www.washingtonpost.com/world/middle_east/iran-president-backs-french-plan-to-restart-talks-with-the-us/2019/10/02/db1cb39e-e4f9-11e9-b403-f738899982d2_story.html (Accessed: 28 April 2021).

Danon, D. (2018) 'Letter from the Permanent Representative of Israel to the United Nations to the Secretary-General and President of the Security Council: code S/2018/495'. Available at: https://undocs.org/pdf?symbol=en/S/2018/495 (Accessed: 16 June 2021).

Davenport, K. (2016) 'Iran's Missile Tests Raise Concerns', *Arms Control Now*, March. Available at: https://www.armscontrol.org/act/2016-03/news/iran%E2%80%99s-missile-tests-raise-concerns (Accessed: 16 June 2021).

Davenport, K. (2017a) 'The P5+1 And Iran Nuclear Deal Alert, February 17', *Arms Control Now*, 17 February. Available at: https://www.armscontrol.org/blog/2017-02-17/p51-iran-nuclear-deal-alert-february-17 (Accessed: 17 June 2021).

Davenport, K. (2017b) 'The UN Report on the Iran Deal Resolution: The Good, the Unclear, and the Troubling', *Arms Control Now*, 29 June. Available at: https://www.armscontrol.org/blog/2017-06-29/un-report-iran-deal-resolution-good-unclear-troubling (Accessed: 26 April 2021).

Davenport, K. (2017c) *UN Security Council Resolutions on Iran*, *Armscontrol.org*. Available at: https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran (Accessed: 16 June 2021).

Davenport, K. (2019) 'Understanding the U.S. Moves on JCPOA Nonproliferation Project Waivers', *Arms Control Now*, 7 May. Available at: https://www.armscontrol.org/blog/2019-05-07/understanding-us-moves-jcpoa-nonproliferation-project-waivers (Accessed: 18 June 2021).

Davenport, K. and Masterson, J. (2020a) 'IAEA Board Passes Resolution on Iran | P4+1 and Iran Nuclear Deal Alert | Arms Control Association', *Arms Control Now*, 19 June. Available at: https://www.armscontrol.org/blog/2020-06/p4-1-iran-nuclear-deal-alert (Accessed: 29 April 2021).

Davenport, K. and Masterson, J. (2020b) 'Iran's Accumulation of Enriched Uranium Slows | Arms Control Association', *Arms Control Now*, 13 November. Available at: https://www.armscontrol.org/blog/2020-11-13/irans-accumulation-enriched-uranium-slows (Accessed: 14 June 2021).

De Luce, D. and Kube, C. (2019) *Iranian-backed hackers stole data from U.S. government contractor*, *NBC News*. Available at:

https://www.nbcnews.com/politics/national-security/iranian-backed-hackers-stole-data-major-u-s-government-contractor-n980986 (Accessed: 2 July 2021).

Dehghanpisheh, B., Hafezi, P. and Aboulenin, A. (2020) 'WRAPUP 3-U.S., Iran draw back from brink but new threats show crisis not over', *Reuters*, 9 January. Available at: https://www.reuters.com/article/iraq-security-idUSL8N29E0Z4 (Accessed: 15 June 2021).

Denning, D. E. (2009) 'Barriers to Entry: Are They Lower for Cyber Warfare?', *IO Journal*, April, pp. 7–10.

Denzin, N. K. and Lincoln, Y. S. (1994) *Handbook of Qualitative Research*. Thousand Oaks: Sage Publications.

Department of Homeland Security (2019) *CISA Statement on Iranian Cybersecurity Threats*, *Department of Homeland Security*. Available at: https://www.dhs.gov/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats (Accessed: 21 April 2021).

Diamond, J. *et al.* (2019) 'Trump says US was "cocked and loaded" to strike Iran before he pulled back - CNNPolitics', *CNN Politcs*, 21 June. Available at: https://edition.cnn.com/2019/06/21/politics/trump-military-strikes-iran/index.html (Accessed: 1 July 2021).

Dinstein, Y. and Dahl, A. W. (2020) *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*. Cham: Springer International Publishing. doi: 10.1007/978-3-030-39169-0.

Director General IAEA (2016a) *Verification and Monitoring in the Islamic Republic of Iran in light of United Nations Security Council Resolution 2231 (2015)*. GOV/INF/2016/1. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/gov-inf-2016-1.pdf.

Director General IAEA (2016b) *Verification and Monitoring in the Islamic Republic of Iran in light of United Nations Security Council Resolution 2231 (2015)*. GOV/2016/8. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/gov-2016-8-derestricted.pdf.

Director General IAEA (2016c) *Verification and Monitoring in the Islamic Republic of Iran in light of United Nations Security Council Resolution 2231 (2015)*. GOV/2016/23. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/16/06/gov2016-23.pdf (Accessed: 21 July 2021).

Director General IAEA (2016d) *Verification and monitoring in the Islamic Republic of Iran in Light of United Nations Security Council resolution 2231 (2015)*. GOV/2016/46. International Atomic Energy Agency. Available at:

https://www.iaea.org/sites/default/files/16/09/gov2016-46.pdf (Accessed: 21 July 2021).

Director General IAEA (2016e) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2016/55. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/16/11/gov2016-55.pdf (Accessed: 21 July 2021).

Director General IAEA (2016f) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/INF/2016/13. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/govinf2016-13.pdf (Accessed: 21 July 2021).

Director General IAEA (2017a) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2017/10. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/gov2017-10.pdf (Accessed: 21 July 2021).

Director General IAEA (2017b) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2017/24. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/gov2017-24.pdf (Accessed: 21 July 2021).

Director General IAEA (2017c) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2017/35. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/gov2017-35.pdf (Accessed: 21 July 2021).

Director General IAEA (2017d) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2017/48. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/17/11/gov2017-48.pdf (Accessed: 21 July 2021).

Director General IAEA (2018a) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2018/24. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/18/06/gov2018-24.pdf (Accessed: 23 July 2021).

Director General IAEA (2018b) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2018/33. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/18/09/gov2018-33.pdf (Accessed: 23 July 2021).

Director General IAEA (2018c) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2018/47. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/18/11/gov2018-47.pdf (Accessed: 23 July 2021).

Director General IAEA (2018d) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2018/7. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/18/03/gov-2018-7-derestricted.pdf.

Director General IAEA (2019a) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2019/10. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/19/03/gov2019-10.pdf (Accessed: 23 July 2021).

Director General IAEA (2019b) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/INF/2019/12. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/19/11/govinf2019-12.pdf.

Director General IAEA (2019c) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2019/55. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/19/11/gov2019-55.pdf (Accessed: 18 June 2021).

Director General IAEA (2019d) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/INF/2019/9. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/19/07/govinf2019-9.pdf (Accessed: 18 June 2021).

Director General IAEA (2020) *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)*. GOV/2020/41. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/20/11/gov2020-41.pdf (Accessed: 21 June 2021).

Director General IAEA, B. W. (2015) *Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran*. GOV/2015/50. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/gov-2015-50-derestr.pdf.

Dragos, Inc (2020) *North American Electric Cyber Threat Perspective*. Cyber Security. Dragos, Inc, p. 17. Available at: https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf?hsCtaTracking=761f6e40-d390-4762-9144-cb4ac00ce695%7C5186bf64-df46-47f0-bc02-d5b3424365b8.

Edwards, B. *et al.* (2017) 'Strategic aspects of cyberattack, attribution, and blame', *Proceedings of the National Academy of Sciences*, 114(11), pp. 2825–2830. doi: 10.1073/pnas.1700442114.

Egloff, F. J. and Smeets, M. (2021) 'Publicly attributing cyber attacks: a framework', *Journal of Strategic Studies*, 0(0), pp. 1–32. doi: 10.1080/01402390.2021.1895117.

Eshel, T. (2016) 'Simorgh First Launch - an Iranian Success or Failure?', *Defense Update*, 24 April. Available at: https://defense-update.com/20160424_simorgh.html (Accessed: 16 June 2021).

EU Commission (2018a) *European Commission acts to protect the interests of EU companies investing in Iran as part of the EU's continued commitment to the JCPOA*, *European Commission - Press releases*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3861 (Accessed: 26 April 2021).

EU Commission (2018b) *European Commission adopts support package for Iran, with a focus on the private sector*, *European Commission - European Commission*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5103 (Accessed: 27 April 2021).

Farrell, H. and Glaser, C. (2016) *The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine*. SSRN Scholarly Paper ID 2836066. Rochester, NY: Social Science Research Network. doi: 10.2139/ssrn.2836066.

Fars News Agency (2020) *Minister: Iran's Pursuit of Space Technology Unstoppable*, *Fars News Agency*. Available at: https://www.farsnews.ir/en/news/13981121000437/Miniser-Iran%E2%80%99s-Prsi-f-Space-Technlgy-Unsppable (Accessed: 29 April 2021).

Fassihi, F. and Gladstone, R. (2019) 'With Brutal Crackdown, Iran Is Convulsed by Worst Unrest in 40 Years', *The New York Times*, 1 December. Available at: https://www.nytimes.com/2019/12/01/world/middleeast/iran-protests-deaths.html (Accessed: 7 July 2021).

Fischerkeller, M. P. and Harknett, R. J. (2019a) 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *Cyber Defense Review*, pp. 261–287.

Fischerkeller, M. P. and Harknett, R. J. (2019b) 'What Is Agreed Competition in Cyberspace?', *Lawfare*, 19 February. Available at:

https://www.lawfareblog.com/what-agreed-competition-cyberspace (Accessed: 8 November 2020).

Fischerkeller, M. P. and Harknett, R. J. (2020) ‘Cyber Persistence, Intelligence Contest, and Strategic Competition’, in. *Policy Roundtable: Cyber Conflict as an Intelligence Contest*, Texas National Security Review. Available at: https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/#essay4.

Fitch, A. and Eqbali, A. (2016) ‘Iran’s President Orders Development of Nuclear-Propulsion System for Ships’, *Wall Street Journal*, 13 December. Available at: https://www.wsj.com/articles/iranian-president-orders-development-of-nuclear-powered-ships-1481652235 (Accessed: 23 July 2021).

Gambrell, J. (2020) *Iran builds at underground nuclear facility amid US tensions*, *AP News*. Available at: https://apnews.com/article/iran-underground-nuclear-facility-d9809b8a61f71f87dff31da6ff784687 (Accessed: 22 June 2021).

Gartzke, E. (2013) ‘The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth’, *International Security*, 38(2), pp. 41–73.

Gartzke, E. and Lindsay, J. R. (2015) ‘Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace’, *Security Studies*, 24(2), pp. 316–348. doi: 10.1080/09636412.2015.1038188.

Gol, J. (2020) ‘Iran blasts: What is behind mysterious fires at key sites?’, *BBC News*, 6 July. Available at: https://www.bbc.com/news/world-middle-east-53305940 (Accessed: 23 July 2021).

Greenberg, A. (2019) ‘A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems’, *Wired*, 20 November. Available at: https://www.wired.com/story/iran-apt33-industrial-control-systems/ (Accessed: 21 April 2021).

Greenberg, A. (2020) ‘Iranian Hackers Have Been “Password-Spraying” the US Grid’, *Wired*, 9 January. Available at: https://www.wired.com/story/iran-apt33-us-electric-grid/ (Accessed: 16 April 2021).

Guarnieri, C. and Anderson, C. (2016) *Iran and the Soft War for Internet Dominance*, p. 57. Available at: https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf.

Hafezi, P. (2020) ‘Iran watchdog passes law on hardening nuclear stance, halting U.N. inspections’, *Reuters*, 3 December. Available at: https://www.reuters.com/article/us-iran-nuclear-law-idUSKBN28C2F7 (Accessed: 14 June 2021).

Hafezi, P. and Stewart, P. (2020) 'Iran says it puts first military satellite into orbit, triggers U.S. condemnation', *Reuters*, 22 April. Available at: https://www.reuters.com/article/us-iran-satellite-idUSKCN2240LO (Accessed: 29 April 2021).

Harknett, R. J. and Goldman, E. (2016) 'The Search for Cyber Fundamentals', *Journal of Information Warfare*, 15(2), pp. 81–88.

Harknett, R. J. and Smeets, M. (2020) 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies*, 0(0), pp. 1–34. doi: 10.1080/01402390.2020.1732354.

Healey, J. (2019) 'The Cartwright Conjecture: The Deterrent Value and Escalatory Risks of Fearsome Cyber Capabilities', in Lin, H. and Zegart, A., *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, D.C., USA: Brooking Institute Press.

Healey, J. and Grindal, K. (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.

Helmhold, J. and Roth, D. J. (2018) *Israel to U.N. Security Council: Iran still testing ballistic missiles*, *The Jerusalem Post | JPost.com*. Available at: https://www.jpost.com/middle-east/iran-news/danon-to-security-council-iran-still-testing-ballistic-missiles-558274 (Accessed: 16 June 2021).

Hinz, F. (2020) *Have Iran's space ambitions taken a worrisome new turn?*, *European Leadership Network*. Available at: https://www.europeanleadershipnetwork.org/commentary/have-irans-space-ambitions-taken-a-worrisome-new-turn/ (Accessed: 29 April 2021).

Hirani, M., Jones, S. and Read, B. (2019) 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', *Threat Research*, 10 January. Available at: https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html (Accessed: 19 April 2021).

Hodgson, Q. *et al.* (2019) *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*. RAND Corporation. doi: 10.7249/RR2961.

Hume, T. (2015) *Iran test-fires new generation long-range missile*, *CNN*. Available at: https://www.cnn.com/2015/10/11/middleeast/iran-ballistic-missile-test/index.html (Accessed: 16 June 2021).

International Atomic Energy Agency (2019) 'Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015)'. International Atomic Energy Agency. Available at: https://www.iaea.org/sites/default/files/19/09/govinf2019-10.pdf.

International Atomic Energy Agency (2020a) *Joint Statement by the Director General of the IAEA and the Vice-President of the Islamic Republic of Iran and Head of the AEOI*, *IAEA.org*. IAEA. Available at: https://www.iaea.org/newscenter/pressreleases/joint-statement-by-the-director-general-of-the-iaea-and-the-vice-president-of-the-islamic-republic-of-iran-and-head-of-the-aeoi (Accessed: 30 April 2021).

International Atomic Energy Agency (2020b) *NPT safeguards agreement with the Islamic Republic of Iran*. GOV/2020/30. International Atomic Energy Agency, p. 4. Available at: https://www.iaea.org/sites/default/files/20/06/gov2020-30.pdf (Accessed: 29 April 2021).

Iran Watch (2020) 'Iran Missile Milestones: 1985-2020', *Iran Watch*. Available at: https://www.iranwatch.org/our-publications/weapon-program-background-report/iran-missile-milestones-1985-2020 (Accessed: 16 June 2021).

Irish, J. and Faulconbridge, G. (2020) 'Britain, France, Germany formally accuse Iran of breaking nuclear deal', *Reuters*, 14 January. Available at: https://www.reuters.com/article/uk-iran-nuclear-idUKKBN1ZD138 (Accessed: 29 April 2021).

IRNA (2021) *Press TV switches to presstv.ir domain after US seizure*, *IRNA English*. IRNA English. Available at: https://en.irna.ir/news/84379356/Press-TV-switches-to-presstv-ir-domain-after-US-seizure (Accessed: 20 July 2021).

Islamic Republic News Agency (2020a) *First ballistic missiles fired deeply from beneath Earth by IRGC*, *IRNA English*. IRNA English. Available at: https://en.irna.ir/news/83889909/First-ballistic-missiles-fired-deeply-from-beneath-Earth-by-IRGC (Accessed: 30 April 2021).

Islamic Republic News Agency (2020b) *Iran takes final step by abandoning JCPOA restrictions*, *IRNA English*. IRNA English. Available at: https://en.irna.ir/news/83622509/Iran-takes-final-step-by-abandoning-JCPOA-restrictions (Accessed: 28 April 2021).

Jaffe, G. and Mufson, S. (2016) 'Obama: Iran nuclear deal, prisoner release show the power of diplomacy', *Washington Post*, 17 January. Available at: https://www.washingtonpost.com/politics/obama-to-speak-to-the-nation-on-iran-at-1045-am/2016/01/17/9ea861a8-bd23-11e5-9443-7074c3645405_story.html (Accessed: 15 June 2021).

Jensen, B. (2017) 'The Cyber Character of Political Warfare', *Brown Journal of World Affairs*, 24(1), pp. 159–171.

Jensen, B. and Valeriano, B. (2019) 'What Do We Know About Cyber Escalation? Observations from Simulations and Surveys', *Issue Brief*. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf.

Jervis, R. (1978) ‘Cooperation Under the Security Dilemma’, *World Politics*, 30(2), pp. 167–214. doi: 10.2307/2009958.

Joint Statement of France, Germany, UK and US (2017) *Iran’s Space Launch Vehicle Inconsistent With UNSCR 2231 Joint Statem…*, *U.S. Department of State Archive*. Available at: http://archive.fo/O47DP (Accessed: 16 June 2021).

Kahn, H. (2017) *On Escalation: Metaphors and Scenarios*. London: Routledge.

Karimi, N. (2020a) *Iran’s parliament approves bill to stop nuclear inspections*, *AP NEWS*. Available at: https://apnews.com/article/iran-parlianment-bill-nuclear-inspection-e2f2225c1f91c5c09afaf776cf9e04e3 (Accessed: 15 June 2021).

Karimi, N. (2020b) *Iran’s Rouhani warns UN agency over nuke site access demands*, *AP NEWS*. Available at: https://apnews.com/article/babf510fb24d9098bb38d95eaa190d4f (Accessed: 29 April 2021).

Karimi, N., Vahdat, A. and Gambrell, J. (2020) *Iran strikes back at US with missile attack at bases in Iraq*, *AP NEWS*. Available at: https://apnews.com/article/ap-top-news-persian-gulf-tensions-tehran-international-news-iraq-add7a702258b4419d796aa5f48e577fc (Accessed: 15 June 2021).

Kaspersky Lab (2021) *Targeted cyberattacks logbook*, *APT Kaspersky Securelist*. Available at: https://apt.securelist.com/# (Accessed: 16 November 2020).

Kello, L. (2017) *The Virtual Weapon and International Order*. Yale University Press. doi: 10.2307/j.ctt1trkjd1.

Khoshnood, A. (2021) ‘ASMLA: An Empirical Exploration of an Ethno-Nationalist Terrorist Organization’, *Mideast Security and Policy Studies*, (193). Available at: https://besacenter.org/asmla-terrorist-organization/.

Kostyuk, N., Powell, S. and Skach, M. (2018) ‘Deternimant of the Cyber Escalation Ladder’, *Cyber Defense Review*, Spring, pp. 123–133.

Krepinevich, A. (2012) *Cyber Warfare: a ‘nuclear option?’* Center for Strategic and Budgetary Assessment, p. 207. Available at: https://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf.

Kreps, S. E. and Schneider, J. (2018) *Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics*. SSRN Scholarly Paper ID 3104014. Rochester, NY: Social Science Research Network. doi: 10.2139/ssrn.3104014.

Kube, C. *et al.* (2018) *Officials: Iran has made preparations for possible cyberattack on U.S.*, *NBC News*. Available at:

https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081 (Accessed: 16 November 2020).

Langner, R. (2013) *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Available at: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Libicki, M. C. (2007) *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press. Available at: https://www.rand.org/pubs/commercial_books/CB407.html (Accessed: 28 May 2021).

Libicki, M. C. (2012) *Crisis and Escalation in Cyberspace*. Santa Monica, UNITED STATES: RAND Corporation, The. Available at: http://ebookcentral.proquest.com/lib/gla/detail.action?docID=1365190 (Accessed: 23 May 2021).

Libicki, M. C. and Tkacheva, O. (2020) 'Cyberspace Escalation: Ladders or Lattices?', in *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallin: NATO CCDCOE Publications, pp. 60–72. Available at: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.

Lin, H. (2012a) 'Escalation Dynamics and Conflict Termination in Cyberspace', *Strategic Studies Quarterly*, 6(3), pp. 46–70.

Lin, H. (2012b) 'Operational Considerations in Cyber Attack and Cyber Exploitation', in *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*. Washington, D.C.: Georgetown University Press.

Lindsay, J. and Gartzke, E. (2016) 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited', in Greenhill, K. m. and Krause, P. J. P., *The Power to Hurt: Coercion in Theory and Practice*. New York: Oxford University Press, pp. 179–203. Available at: https://www.semanticscholar.org/paper/Coercion-through-Cyberspace-%3A-The-Paradox-Revisited-Lindsay-Gartzke/78b8e7abf96e4ab276dc05a91beab4055fba9836.

Lindsay, J. R. (2013) 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22(3), pp. 365–404. doi: https://doi-org.ezproxy.lib.gla.ac.uk/10.1080/09636412.2013.816122.

Lindsay, J. R. (2015) 'Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack', *Journal of Cybersecurity*, 1(1), pp. 53–67. doi: 10.1093/cybsec/tyv003.

Lindsay, J. R. (2020) 'Military Organizations, Intelligence Operations, and Information Technology', in. *Policy Roundtable: Cyber Conflict as an Intelligence Contest*, Texas National Security Review. Available at:

https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/#essay3.

Litvak, P. and Kajiloti, M. (2020) 'Intezer - New Iranian Campaign Tailored to US Companies Uses Updated Toolset', *Intezer*, 30 January. Available at: https://www.intezer.com/blog/malware-analysis/new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/ (Accessed: 21 April 2021).

Lyngaas, S. (2020a) *Iranian hackers probed election-related websites in 10 states, US officials say*, *CyberScoop*. Available at: https://www.cyberscoop.com/iran-election-hacking-state-websites-probe-fbi/ (Accessed: 9 April 2021).

Lyngaas, S. (2020b) *US Treasury sanctions 5 Iranian organizations for alleged election influence operations*, *CyberScoop*. Available at: https://www.cyberscoop.com/iran-treasury-sanctions-irgc-elections/ (Accessed: 5 July 2021).

Lynn, W. J. (2010) 'Defending a New Domain', September. Available at: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (Accessed: 29 May 2021).

Lynn-Jones, S. M. (1995) 'Offense-Defense Theory and Its Critics', *Security Studies*, 4(4), pp. 660–691.

Macias, A. (2019) *Trump sanctions Iranian metals, Tehran's largest non-petroleum-related sources of export revenue*, *CNBC*. Available at: https://www.cnbc.com/2019/05/08/trump-sanctions-iranian-exports-of-steel-copper-and-other-metals.html (Accessed: 18 June 2021).

Majd, H. (2008) *The Ayatollah begs to differ: the paradox of modern Iran*. 1. ed. New York: Doubleday.

Maksh, M. (2020) *CISA, FBI Warn Iran-based Threat Actor May Be Planning Ransomware Attacks*, *Nextgov.com*. Available at: https://www.nextgov.com/cybersecurity/2020/09/cisa-fbi-warns-iran-based-threat-actor-may-be-planning-ransomware-attacks/168520/ (Accessed: 9 April 2021).

Managan, D., Breuninger, K. and Kimball, S. (2020) *Iran and Russia obtained U.S. voter registration data in effort to influence election, national security officials say*, *CNBC*. Available at: https://www.cnbc.com/2020/10/21/fbi-to-make-an-announcement-on-a-major-election-security-issue.html (Accessed: 23 April 2021).

Martinez, L. and McLaughlin, E. (2020) *Iran launches missiles at US military facilities in Iraq, Pentagon confirms*, *ABC News*. Available at: https://abcnews.go.com/International/iran-launches-missiles-us-air-bases-iraq-us/story?id=68130625 (Accessed: 17 June 2021).

Mattis, J. (2018) ‘Summary of the 2018 National Defense Strategy’. United States Department of Defense. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Maurer, T. (2018) *Cyber mercenaries: the state, hackers, and power*. Cambridge New York, NY Port Melbourne New Delhi Singapore: Cambridge University Press.

McConnell, M. (2009) ‘Cyberwar Is the New Atomic Age’, *New Perspectives Quarterly*, 26(3), pp. 72–77. doi: https://doi.org/10.1111/j.1540-5842.2009.01103.x.

McLaughlin, J., Dorfman, Z. and Naylor, S. D. (2019) *Pentagon secretly struck back against Iranian cyberspies targeting U.S. ships*, *Yahoo News*. Available at: https://news.yahoo.com/pentagon-secretly-struck-back-against-iranian-cyber-spies-targeting-us-ships-234520824.html (Accessed: 20 April 2021).

McMillan, R. (2020) ‘Presidential Campaigns Targeted by Suspected Chinese, Iranian Hackers’, *Wall Street Journal*, 4 June. Available at: https://www.wsj.com/articles/presidential-campaigns-targeted-by-suspected-chinese-iranian-hackers-11591294980 (Accessed: 12 April 2021).

Mehr News Agency (2020) *Over 80 killed in IRGC’s missile strikes on US airbases in Iraq: Informed source*, *Mehr News Agency*. Mehr News Agency. Available at: https://en.mehrnews.com/news/154310/Over-80-killed-in-IRGC-s-missile-strikes-on-US-airbases-in-Iraq (Accessed: 17 June 2021).

Middle East Monitor (2020) *Iran parliament approves bill on uranium enrichment*, *Middle East Monitor*. Available at: https://www.middleeastmonitor.com/20201103-iran-parliament-approves-bill-on-uranium-enrichment/ (Accessed: 14 June 2021).

Mizokami, K. (2017) *Pentagon: Iran Tested a Ballistic Missile With North Korean Origins*, *Popular Mechanics*. Available at: https://www.popularmechanics.com/military/weapons/a24986/iran-missile-north-korea/ (Accessed: 16 June 2021).

Momtaz, R. (2019) *Trump, Rouhani agreed 4-point plan before Iran balked: French officials*, *POLITICO*. Available at: https://www.politico.eu/article/trump-rouhani-agreed-4-point-plan-before-iran-balked-french-officials/ (Accessed: 28 April 2021).

Morgan, F. E. *et al.* (2008) *Dangerous Thresholds: Managing Escalation in teh 21st Century*. Santa Monica, CA: RAND Corporation.

Mostaghim, R. and McDonnell, P. (2016) *Iran’s latest missile test launches do not violate nuclear deal, U.S. says*, *Los Angeles Times*. Available at:

https://www.latimes.com/world/la-fg-iran-missiles-20160309-story.html (Accessed: 16 June 2021).

Motamedi, M. (2020) *Rouhani: 'No negotiations' needed to restore Iran nuclear deal*, *Al Jaseera English*. Available at: https://www.aljazeera.com/news/2020/12/9/iran-rouhani-no-negotiations-on-nuclear-deal (Accessed: 15 June 2021).

Murdock, J. (2018) *Hackers are now targeting U.S. power grid companies—will there be blackouts?*, *Newsweek*. Available at: https://www.newsweek.com/what-raspite-us-electric-grids-under-threat-new-hacking-group-1054053 (Accessed: 12 April 2021).

Murphy, F. (2020) 'Iran feeds uranium gas into advanced centrifuges underground -IAEA report', *Reuters*, 18 November. Available at: https://www.reuters.com/article/iran-nuclear-iaea-int-idUSKBN27Y0W5 (Accessed: 14 June 2021).

Nakashima, E. (2019) 'Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers', *Washington Post*, 22 June. Available at: https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html (Accessed: 9 April 2021).

Nichols, M. (2020) 'U.N. chief says no action on U.N. Iran sanctions due to "uncertainty"', *Reuters*, 20 September. Available at: https://www.reuters.com/article/us-iran-usa-un-idUSKCN26B03X (Accessed: 14 June 2021).

Nichols, S. (2019) *Iranian-backed hackers ransacked Citrix, swiped 6TB+ of emails, docs, secrets, claims cyber-biz*, *The Registrer*. Available at: https://www.theregister.com/2019/03/08/citrix_hacked_data_stolen/ (Accessed: 2 July 2021).

O'Donnell, L. (2019) *Iran-Linked APT33 Shakes Up Cyberespionage Tactics*, *Threat Post*. Available at: https://threatpost.com/iranian-apt33-shakes-up-cyberespionage-tactics/146041/ (Accessed: 9 April 2021).

Office of the President of Iran (2019) *Iran's third step to begin Friday; Atomic Energy Org. authorized to do whatever needed in nuclear technology, research*, *Office of the President of Iran*. Available at: http://president.ir/en/111155 (Accessed: 28 April 2021).

O'Flaherty, K. (2019) *Iranian Hackers Are Going After A Disturbing New Physical Target*, *Forbes*. Available at: https://www.forbes.com/sites/kateoflahertyuk/2019/11/21/iranian-hackers-could-be-going-after-a-disturbing-new-physical-target/ (Accessed: 9 April 2021).

O'Flaherty, K. (2020) 'The Iran Cyber Warfare Threat: Everything You Need To Know', *Forbes*, 6 January. Available at: https://www.forbes.com/sites/kateoflahertyuk/2020/01/06/the-iran-cyber-warfare-threat-everything-you-need-to-know/ (Accessed: 10 December 2020).

Owen, T. and Francheschi-Bicchieria, L. (2020) *'Proud Boys' Emails Threatening Florida Voters Appear to Use Spoofed Email Address*, *Motherboard: Tech by Vice*. Available at: https://www.vice.com/en/article/88a43b/proud-boys-emails-threatening-florida-voters-appear-to-use-spoofed-email-address (Accessed: 5 July 2021).

Pamuk, H. and Irish, J. (2020) 'U.S. renews waivers on Iran nuclear work, but sanctions top Iran nuclear official', *Reuters*, 30 January. Available at: https://www.reuters.com/article/us-iran-nuclear-usa-idUSKBN1ZT1PW (Accessed: 29 April 2021).

Perlroth, N. (2017) 'Web Defenders Detect Russian Hand in Iranians' Hacking Attempt', *The New York Times*, 15 May. Available at: https://www.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html (Accessed: 12 April 2021).

Perlroth, N. (2019) 'Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies', *The New York Times*, 18 February. Available at: https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html (Accessed: 19 April 2021).

Perlroth, N. and Sanger, D. E. (2019) 'Iranian Hackers Target Trump Campaign as Threats to 2020 Mount', *The New York Times*, 4 October. Available at: https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html (Accessed: 12 April 2021).

Pražák, J. (2021) 'Dual-use conundrum: Towards the weaponization of outer space? (forthcoming)', *Acta Astronautica*. doi: 10.1016/j.actaastro.2020.12.051.

PressTV (2018) *Iran's IAEA envoy: Tehran to restart nuclear activities if JCPOA fails*, *PressTV*. PressTV. Available at: https://www.presstv.com/Detail/2018/06/06/564126/Iran-nuclear-deal-US-JCPOA-Board-of-Governors-Reza-Najafi (Accessed: 27 April 2021).

PressTV (2020) *Iran to increase nuclear power capacity to 3GW: Minister*, *PressTV*. PressTV. Available at: https://www.presstv.com/Detail/2020/10/04/635653/Iran-nuclear-power-generation-Ardakanian-announcement (Accessed: 14 June 2021).

Priyanka R (2020) 'FBI warns about Iranian hacking group attacking F5 networking devices | Cybersafe News', *Cyber Hacking News*, 10 August. Available at: https://www.cybersafe.news/fbi-warns-about-iranian-hacking-group-attacking-f5-networking-devices/ (Accessed: 19 April 2021).

Radio Farda (2020) *Security Website Says Incident At Iran's Nuclear Plant Was 'Deliberate Attack'*, *Radio Farda*. Available at: https://en.radiofarda.com/a/security-website-says-incident-at-iran-s-nuclear-plant-was-deliberate-attack-/30712034.html (Accessed: 29 April 2021).

Reichborn-Kjennerud, E. and Cullen, P. (2016) *What is Hybrid Warfare?* Policy Brief 1/2016. Oslo: Norwegian institute of international affairs (NUPI), p. 4. Available at: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf?sequence=3&isAllowed=y (Accessed: 1 December 2020).

Reuters (2018) 'Iran builds new centrifuge rotor factory: nuclear chief', *Reuters*, 18 July. Available at: https://www.reuters.com/article/us-iran-nuclear-centrifuge-idUSKBN1K80OP (Accessed: 26 April 2021).

Reuters (2020) 'Iran building new production hall for centrifuges in mountains near Natanz', *Reuters*, 8 September. Available at: https://www.reuters.com/article/us-iran-nuclear-natanz-idUSKBN25Z239 (Accessed: 14 June 2021).

Rid, T. (2012) 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35(1), pp. 5–32. doi: 10.1080/01402390.2011.608939.

Rid, T. and Buchanan, B. (2015) 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38(1–2), pp. 4–37. doi: 10.1080/01402390.2014.977382.

Rising, D. (2020) *UN watchdog: Iran building at underground nuclear facility*, *Associated Press*. Available at: https://apnews.com/article/united-nations-donald-trump-iran-middle-east-europe-effcfe5ea7d691b471355a4b49c7a18c (Accessed: 14 June 2021).

Rovner, J. (2019) 'Cyber War as an Intelligence Contest', *War on the Rocks*, 16 September. Available at: https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/ (Accessed: 14 October 2020).

Royce, E. R. (2017) *H.R.3364 - 115th Congress (2017-2018): Countering America's Adversaries Through Sanctions Act*, *H.R.3364*. Available at: https://www.congress.gov/bill/115th-congress/house-bill/3364 (Accessed: 15 June 2021).

Sanger, D. E. (2016) 'Iran Complies With Nuclear Deal; Sanctions Are Lifted', *The New York Times*, 16 January. Available at: https://www.nytimes.com/2016/01/17/world/middleeast/iran-sanctions-lifted-nuclear-deal.html (Accessed: 15 June 2021).

Sanger, D. E. (2017) 'Iran Launches a Missile, Testing Trump's Vows of Strict Enforcement', *The New York Times*, 30 January. Available at:

https://www.nytimes.com/2017/01/30/world/middleeast/iran-missile-test.html (Accessed: 16 June 2021).

Sanger, D. E. and Perlroth, N. (2015) ‘Iranian Hackers Attack State Dept. via Social Media Accounts’, *The New York Times*, 24 November. Available at: https://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html (Accessed: 20 April 2021).

SBS (2018) *Iran says it will retaliate after ‘hostile’ US sanctions amid nuclear deal tensions*, *SBS News*. Available at: https://www.sbs.com.au/news/iran-says-it-will-retaliate-after-hostile-us-sanctions-amid-nuclear-deal-tensions/f0b90091-a963-4724-9cf0-8b50aadc09f7 (Accessed: 19 April 2021).

Schelling, T. C. (1967) *Arms and Influence*. Hartford, UNITED STATES: Yale University Press. Available at: http://ebookcentral.proquest.com/lib/gla/detail.action?docID=3421294 (Accessed: 24 May 2021).

Schmerler, D. (2019) ‘Iran’s Space Launch: ICBM or Space Program Development?’, *Foreign Policy Research Institute*, 22 January. Available at: https://www.fpri.org/article/2019/01/irans-space-launch-icbm-or-space-program-development/ (Accessed: 17 June 2021).

Schmitt, E. and Sanger, D. E. (2019) ‘In Escalation, Iran Tests Medium-Range Missile, U.S. Official Says’, *The New York Times*, 26 July. Available at: https://www.nytimes.com/2019/07/25/us/politics/iran-missile-test.html (Accessed: 17 June 2021).

Sharp, T. (2017) ‘Theorizing cyber coercion: The 2014 North Korean operation against Sony’, *Journal of Strategic Studies*, 40(7), pp. 898–926. doi: 10.1080/01402390.2017.1307741.

Smeets, M. (2018a) ‘A matter of time: On the transitory nature of cyberweapons’, *Journal of Strategic Studies*, 41(1–2), pp. 6–32. doi: 10.1080/01402390.2017.1288107.

Smeets, M. (2018b) ‘The Strategic Promise of Offensive Cyber Operations’, *Strategic Studies Quarterly*, 12(3), pp. 90–113.

Solomon, J. (2015) ‘U.S. Detects Flurry of Iranian Hacking’, *Wall Street Journal*, 5 November. Available at: https://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754 (Accessed: 13 April 2021).

Solomon, J. and Fassihi, F. (2015) ‘Iranian-American Executive Arrested in Iran’, *Wall Street Journal*, 30 October. Available at: https://www.wsj.com/articles/iranian-american-executive-arrested-in-iran-1446164677 (Accessed: 24 April 2021).

State of Georgia, USA (2018) *Atlanta U.S. Attorney Charges Iranian nationals for City Of Atlanta ransomware attack*. Available at: https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack (Accessed: 21 April 2021).

Swan, B. and Rawnsley, A. (2019) 'EXCLUSIVE: Trump Admin Inflated Iran Intel, U.S. Officials Say', *The Daily Beast*, 8 May. Available at: https://www.thedailybeast.com/trump-administration-inflated-iran-intelligence-us-officials-say (Accessed: 27 April 2021).

Tabatabai, A. M. (2018) 'Other side of the Iranian coin: Iran's counterterrorism apparatus', *Journal of Strategic Studies*, 41(1–2), pp. 181–207. doi: 10.1080/01402390.2017.1283613.

Tabatabai, A. M. (2020) *No conquest, no defeat: Iran's national security strategy*. London: Hurst & Company.

Takahashi, S. (2018) 'Development of gray-zone deterrence: concept building and lessons from Japan's experience', *The Pacific Review*, 31(6), pp. 787–810. doi: 10.1080/09512748.2018.1513551.

Talmazan, Y. and Arouzi, A. (2021) *U.S. seizes Iran-linked websites, alleging disinformation*, *NBC News*. Available at: https://www.nbcnews.com/news/world/u-s-seizes-over-30-websites-linked-iranian-disinformation-n1272076 (Accessed: 20 July 2021).

Tehran Times (2018) *Ayatollah Khamenei sets seven conditions for Europe to save nuclear deal*, *Tehran Times*. Available at: https://www.tehrantimes.com/news/423907/Ayatollah-Khamenei-sets-seven-conditions-for-Europe-to-save-nuclear (Accessed: 17 June 2021).

Tehran Times (2020) *Parliament prepares plan to stop Additional Protocol in Iran*, *Tehran Times*. Available at: https://www.tehrantimes.com/news/449878/Parliament-prepares-plan-to-stop-Additional-Protocol-in-Iran (Accessed: 30 April 2021).

The Defense Post (2019) 'Iran successfully flight tests Hoveizeh long-range cruise missile', *The Defense Post*, 2 February. Available at: https://www.thedefensepost.com/2019/02/02/iran-hoveizeh-cruise-missile-test-successful/ (Accessed: 17 June 2021).

The White House (2017a) 'National Security Strategy of teh United States of America'. Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (Accessed: 29 May 2021).

The White House (2017b) *Press Briefing by Principal Deputy Press Secretary Sarah Sanders and Director of Legislative Affairs Marc Short – The White House*, *Trump White House Archives*. Available at: https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-principal-deputy-press-secretary-sarah-sanders-director-legislative-affairs-marc-short-071017/ (Accessed: 16 June 2021).

Times of Israel and Associted Press (2016) *Iran conducts 4th missile test since signing nuke deal*. Available at: http://www.timesofisrael.com/iran-conducts-4th-missile-test-since-signing-nuke-deal/ (Accessed: 16 June 2021).

Turak, N. (2020) *Iranian hackers are targeting state election websites and accessing voter data, FBI says*, *CNBC*. Available at: https://www.cnbc.com/2020/10/31/fbi-iranian-hackers-are-targeting-state-election-websites-voter-data.html (Accessed: 9 April 2021).

United Against a Nuclear Iran (2018) *Thank You for Making the 2018 Iran Summit a Success*, *United Against a Nuclear Iran*. Available at: https://www.unitedagainstnucleariran.com/press-releases/thank-you-for-making-2018-iran-summit-success (Accessed: 27 April 2021).

United Nations Secretary-General (2017) *Third report of the Secretary-General on the implementation of Security Council resolution 2231 (2015)*. S/2017/551. New York City: United Nations Security Council, p. 9. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/167/39/PDF/N1716739.pdf?OpenElement (Accessed: 26 April 2021).

United Nations Secretary-General (2020) *Implementation of Security Council resolution 2231 (2015): Ninth report of the Secretary-General*. S/2020/531. United Nations Security Council, p. 12. Available at: https://www.undocs.org/pdf?symbol=en/S/2020/531 (Accessed: 29 April 2021).

United Nations Security Council (2010) *Resolution 1929 (2010). Adopted by the security council at its 6335th meeting, on 9 June 2010*. Available at: https://www.iaea.org/sites/default/files/unsc_res1929-2010.pdf (Accessed: 16 June 2021).

United Nations Security Council (2015) *Resolution 2231 (2015) Adopted by the Security Council at its 7488th meeting, on 20 July 2015*. Available at: https://www.undocs.org/pdf?symbol=en/S/RES/2231(2015) (Accessed: 17 June 2021).

United States Department of State (2020) 'Sweeping U.S. Measures to Support Return of UN Sanctions Relating to Iran's Nuclear, Missile, and Conventional Arms Programs', *United States Department of State*, 21 September. Available at: https://2017-2021.state.gov/sweeping-u-s-measures-to-support-return-of-un-sanctions-relating-to-irans-nuclear-missile-and-conventional-arms-programs/ (Accessed: 14 June 2021).

United States Department of Defense (2018) ‘Summary of the Department of Defense Cyber Strategy’. United States Government. Available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Accessed: 29 May 2021).

United States Department of Justice (2021) *United States Seizes Websites Used by the Iranian Islamic Radio and Television Union and Kata’ib Hizballah*. Available at: https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib (Accessed: 20 July 2021).

United States Department of State (2017) *U.S. Announces New Iran-related Sanctions - Press Release*, *United States Department of State*. Available at: https://2017-2021.state.gov/u-s-announces-new-iran-related-sanctions/ (Accessed: 26 April 2021).

United States Department of State (2018a) ‘Background Briefing on President Trump’s Decision To Withdraw From the JCPOA’, *United States Department of State*, 8 May. Available at: https://2017-2021.state.gov/background-briefing-on-president-trumps-decision-to-withdraw-from-the-jcpoa/ (Accessed: 26 April 2021).

United States Department of State (2018b) ‘Constraining Iran’s Nuclear Program’, *United States Department of State*, 5 November. Available at: https://2017-2021.state.gov/constraining-irans-nuclear-program/ (Accessed: 27 April 2021).

United States Department of State (2018c) *Press Availability With Secretary of Treasury Steven T. Mnuchin*, *United States Department of State*. Available at: https://2017-2021.state.gov/press-availability-with-secretary-of-treasury-steven-t-mnuchin/ (Accessed: 27 April 2021).

United States Department of State (2019a) ‘Advancing the Maximum Pressure Campaign by Restricting Iran’s Nuclear Activities’, *United States Department of State*, 3 May. Available at: https://2017-2021.state.gov/advancing-the-maximum-pressure-campaign-by-restricting-irans-nuclear-activities/ (Accessed: 27 April 2021).

United States Department of State (2019b) ‘Findings Pursuant to the Iran Freedom and Counter-Proliferation Act (IFCA) of 2012’, *United States Department of State*, 31 October. Available at: https://2017-2021.state.gov/findings-pursuant-to-the-iran-freedom-and-counter-proliferation-act-ifca-of-2012/ (Accessed: 28 April 2021).

United States Department of State (2019c) *New Sanctions Designations on Iran’s Space Program*, *United States Department of State*. Available at: https://2017-2021.state.gov/new-sanctions-designations-on-irans-space-program/ (Accessed: 28 April 2021).

United States Department of State (2019d) *Rewards for Justice - Reward offer for information on the financial mechanisms of Iran's Islamic Revolutionary Guard Corps and its branches, including the IRGC-Qods Force*, *United States Department of State*. Available at: https://2017-2021.state.gov/rewards-for-justice-reward-offer-for-information-on-the-financial-mechanisms-of-irans-islamic-revolutionary-guard-corps-and-its-branches-including-the-irgc-qods-force/ (Accessed: 28 April 2021).

United States Department of State (2019e) *Sanctioning of Vast IRGC-QF Petroleum Shipping Network*, *United States Department of State*. Available at: https://2017-2021.state.gov/sanctioning-of-vast-irgc-qf-petroleum-shipping-network/ (Accessed: 28 April 2021).

United States Department of State (2019f) 'Secretary Pompeo Tightens Nuclear Restrictions on Iran', *United States Department of State*, 3 May. Available at: https://2017-2021.state.gov/secretary-pompeo-tightens-nuclear-restrictions-on-iran/ (Accessed: 27 April 2021).

United States Department of State (2019g) 'U.S. Sanctions Iran's Central Bank, National Development Fund, and Etemad Tejarat Pars', *United States Department of State*, 20 September. Available at: https://2017-2021.state.gov/u-s-sanctions-irans-central-bank-national-development-fund-and-etemad-tejarat-pars/ (Accessed: 28 April 2021).

United States Department of State (2020a) 'IRGC-QF Sanctions and Iraq's Electricity Waiver', *United States Department of State*, 26 March. Available at: https://2017-2021.state.gov/irgc-qf-sanctions-and-iraqs-electricity-waiver/ (Accessed: 29 April 2021).

United States Department of State (2020b) 'The Return of UN Sanctions on the Islamic Republic of Iran', *United States Department of State*, 19 September. Available at: https://2017-2021.state.gov/the-return-of-un-sanctions-on-the-islamic-republic-of-iran/ (Accessed: 14 June 2021).

United States Department of the Treasury (2018) *Statement by Secretary Steven T. Mnuchin on Iran Decision*, *U.S. Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/sm0382 (Accessed: 27 April 2021).

United States Department of the Treasury (2019) *Treasury Designates Vast Iranian Petroleum Shipping Network That Supports IRGC-QF and Terror Proxies*, *U.S Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/sm767 (Accessed: 28 April 2021).

United States Department of the Treasury (2020a) *Treasury Sanctions Iranian Entities for Attempted Election Interference*, *U.S. Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/sm1158 (Accessed: 5 July 2021).

United States Department of the Treasury (2020b) *Treasury Sanctions Key Actors in Iran's Oil Sector for Supporting Islamic Revolutionary Guard Corps-Qods Force*, *United States Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/sm1165 (Accessed: 14 June 2021).

Vahdat, A. and Gambrell, J. (2020) *In latest message to US, Iran launches underground ballistic missiles during exercise targeting mock carrier*, *Military Times*. Available at: https://www.militarytimes.com/news/your-military/2020/07/29/in-latest-message-to-us-iran-launches-underground-ballistic-missiles-during-exercise-targeting-mock-carrier/ (Accessed: 17 June 2021).

Valeriano, B., Jensen, B. and Maness, R. C. (2018) *Cyber Strategy: The Evolving Character of Power and Coercion*, *Cyber Strategy*. New York, N.Y.: Oxford University Press. Available at: https://oxford-universitypressscholarship-com.ezproxy.lib.gla.ac.uk/view/10.1093/oso/9780190618094.001.0001/oso-9780190618094 (Accessed: 19 May 2021).

Valeriano, B. and Maness, R. C. (2014) 'The dynamics of cyber conflict between rival antagonists, 2001–11', *Journal of Peace Research*, 51(3), pp. 347–360. doi: 10.1177/0022343313518940.

Van der Berg, S. and Sterling, T. (2018) 'World Court hears Iran lawsuit to have U.S. sanctions lifted', *Reuters*, 27 August. Available at: https://www.reuters.com/article/us-iran-nuclear-usa-sanctions-idUSKCN1LC00G (Accessed: 27 April 2021).

Van Puyvelde, D. and Brantly, A. F. (2019) *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Cambridge, UK: Polity Press.

Vavra, S. (2019) *Why Cyber Command's latest warning is a win for the government's information sharing efforts*, *CyberScoop*. Available at: https://www.cyberscoop.com/cyber-command-information-sharing-virustotal-iran-russia/ (Accessed: 12 April 2021).

Vavra, S. and Lyngaas, S. (2020) *Why the US was so fast to blame Iran for voter intimidation emails in Florida*, *CyberScoop*. Available at: https://www.cyberscoop.com/ratcliffe-fbi-iran-proud-boys-voting-email/ (Accessed: 5 July 2021).

Wall, M. (2020) *Iran satellite launch fails to reach orbit*, *Space.com*. Available at: https://www.space.com/iran-satellite-launch-failure-zafar-1.html (Accessed: 17 June 2021).

Warner, M. (2002) 'Wanted: A Definition of "Intelligence": Understanding Our Craft', *Studies in Intelligence*, 46(3), pp. 15–22.

Warner, M. (2019) 'A Matter of Trust: Covert Action Reconsidered', 63(4), p. 10.

Watling, J. (2020) ‘Spare Me Your Cyber-Age Technobabble’, *RUSI*, 5 June. Available at: https://rusi.org/publication/rusi-defence-systems/spare-me-your-cyber-age-technobabble (Accessed: 28 May 2021).

Wendling, M. (2020) ‘US Election 2020: Who are the Proud Boys - and who are antifa?’, *BBC News*, 30 September. Available at: https://www.bbc.com/news/election-us-2020-54352635 (Accessed: 23 July 2021).

Wendt, A. (1999) *Social Theory of International Politics*. Cambridge, UK: Cambridge University Press (Cambridge Studies in International Relations). Available at: http://ebookcentral.proquest.com/lib/gla/detail.action?docID=144678 (Accessed: 27 May 2021).

Whyte, C. (2016) ‘Ending cyber coercion: Computer network attack, exploitation and the case of North Korea’, *Comparative Strategy*, 35(2), pp. 93–102. doi: 10.1080/01495933.2016.1176453.

Wilkin, S. (2015) ‘Iran tests new precision-guided ballistic missile’, *Reuters*, 11 October. Available at: https://www.reuters.com/article/us-iran-military-missiles-idUSKCN0S505L20151011 (Accessed: 16 June 2021).

Wintour, P. (2018) *Iran missile tests may breach UN resolution, France and UK warn*, *the Guardian*. Available at: http://www.theguardian.com/world/2018/dec/03/iran-missile-tests-may-breach-un-resolution-france-uk-warn (Accessed: 17 June 2021).

Wroughton, L. and Hafezi, P. (2019) ‘In unprecedented move, U.S. names Iran’s Revolutionary Guards a terrorist group’, *Reuters*, 9 April. Available at: https://www.reuters.com/article/us-usa-iran-idUSKCN1RK1NY (Accessed: 1 July 2021).

Xinhua (2019) *Iran begins installation of IR6 centrifuges: report - Xinhua | English.news.cn*, *Xinhua News*. Available at: http://www.xinhuanet.com/english/2019-04/09/c_137962596.htm (Accessed: 23 July 2021).

Yin, R. K. (2003) *Case Study Research: Design and Methods*. 3rd edition. London: Sage Publications (Applied Social Research Methods Series).

Zetter, K. (2015) *Countdown to Zero Day: Stuxnet and the launch of the world’s first digital weapon*. New York: Crown Publishers.

Appendix A - Data set of cyber operations

Month-year	Description	Target country, sector	Assumed aim	Success	Context block
Oct. 2020	Targeting US State election sites (Lyngaas, 2020a; Managan, Breuninger and Kimball, 2020; Turak, 2020)	United States, Public sector	Espionage, election interference through voter intimidation	One reported breach and an attributed voter intimidation campaign, likely building on data obtained through such breaches	No.5
Sept. 2020	Probing public and private networks through VPN vulnerabilities (Cybersecurity and Infrastructure Security Agency, 2020a; Maksh, 2020)	United States, Public and Private sectors	Espionage, potentially planning ransomware attack	No reports of success	No.5
Aug. 2020	Fox Kitten campaign - Probing major companies and government agencies (Cimpanu, 2020a; Priyanka R, 2020)	United States, Public and Private sectors	Espionage	Partial success, but only breached private companies	No.5
May-Jun. 2020	Targeting the personal accounts of people in the Trump campaign (Burt, 2020; McMillan, 2020)	United States, Public sector	Espionage, election interference	No reports of success	No.5
Jan. 2020	Password spraying attacks against the U.S. electric grid (Dragos, Inc,	United States, public sector	Espionage, possibly preparing physical attack	No reports of success	No.5

	2020; Greenberg, 2020)				
Jan. 2020	Spear phishing campaign impersonating Westat, a client of the Federal Government (Cimpanu, 2020b; Litvak and Kajiloti, 2020)	United States, private and public sectors	Espionage against private company and possibly public clients	Partial success, with an unknown number of federal systems compromised. No reports of further implications.	No.5
Nov. 2019	Password spraying attacks against 2000 organizations, focusing since October 2019 on 200 companies, half of the top 25 of which were in the supply chain of industrial control systems (Greenberg, 2019; O'Flaherty, 2019)	United States, private sector	Espionage, possible preparing supply chain attacks	No reports of success	No.4
Aug.-Sept. 2019	Attempts to breach the email accounts of current and former government officials, civil society actors and people in the Trump presidential campaign (Burt, 2019; Perlroth and Sanger, 2019)	United States, public and civil sectors	Espionage, democratic process	Successful in breaching four accounts, none of which tied to US government or Trump campaign	No.4
Jun. 2019	A spear phishing campaign against companies and government officials (Abdollah, 2019; Barnes and Gibbons-Neff,	United States, public and private sectors	Espionage, CISA says possibly to deploy wiper malware	No reports of success	No.4

	2019; Department of Homeland Security, 2019; O'Donnell, 2019; Vavra, 2019)				
Jan. 2019	A wave of hackingefforts against over half a dozen US federal agencies and several private companies (Hirani, Jones and Read, 2019; Perlroth, 2019)	United States, public and private	Espionage – no data stolen or disruption in activities	No reports of success	No.3
Dec. 2018 & Mar. 2019	US company Citrix was breached twice, leading to 6TB of data being stolen. Citrix had customers in the US military, and government sectors (De Luce and Kube, 2019; Nichols, 2019).	United States, public and private	Data theft	Partial success, but no reports of breaching government systems	No.3
Oct. 2018	Iranian APT target US employees tasked with re-instating sanctions in phishing campaign, including civil society actors globally (Certfa Lab, 2018)	United States and others, public and civil sectors	Espionage	No reports of success	No.3
Jul. 2018	Global campaign targeting electric companies by stealing login information (Kube *et al.*, 2018; Murdock, 2018)	United States, Europe, East Asia and Middle East, private sector	Espionage, possibly to prepare sabotage	No reports of success	No.3
Apr. 2017	Attempted hack of a military	United States,	Espionage	No reports of success	No.2

	contractor (Perlroth, 2017)	private sector			
Nov. 2015	Hack of social media and email accounts of government officials working on Iran issues (Sanger and Perlroth, 2015; Solomon, 2015)	United States, public sector	Espionage, personnel reconnaissance, potentially sabotage of deal	Succeeded in gaining access	No.1