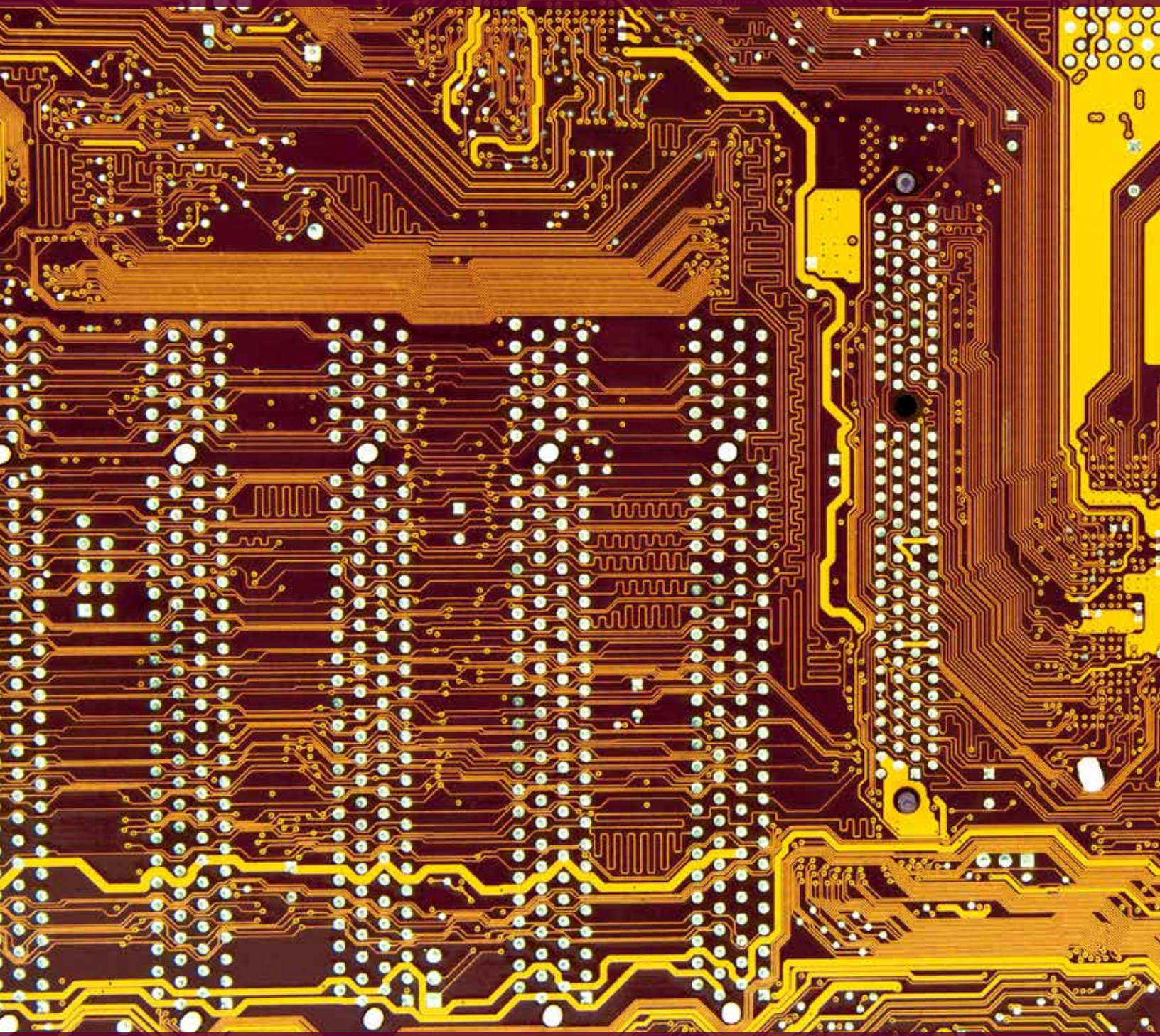
Non-Linear Stratagems in Theory and Practice:
Examples from Iranian Cyber Policies

Ariya Hagh and Peyman Majidzadeh



IRAN MEDIA PROGRAM
پژوهش رسانه در ایران

Annenberg SCHOOL FOR COMMUNICATION
UNIVERSITY of PENNSYLVANIA

About the Authors

Ariya Hagh is a Ph.D. candidate in the Department of Government at Georgetown University, where he specializes in international security, formal theory, and quantitative methodology. His research examines the evolution of autocratic regimes, with a substantive focus on succession dynamics.

Peyman Majidzadeh is a doctoral candidate in Law, Politics, and Development at Scuola Superiore Sant'Anna in Pisa, Italy, and a visiting scholar at Georgetown University. He conducts research on international sanctions, political cohesion and regime survival.

The Iran Media Program is a collaborative network designed to enhance the understanding of Iran's media ecology. Our goal is to strengthen a global network of Iranian media scholars and practitioners and to contribute to Iran's civil society and the wider policy-making community by providing a more nuanced understanding of the role of media and the flow of information in Iran.

The authors would like to thank the Annenberg School for Communication at the University of Pennsylvania, whose support made the development of this paper possible.

Iran Media Program
Annenberg School for Communication
University of Pennsylvania
3620 Walnut St. Philadelphia, PA 19104
Phone: (215) 898 9727
Fax: (215) 573 2609
iranmedia@asc.upenn.edu
www.iranmediaresearch.org

Contents

Executive Summary

In this report, we explore the emergence of a host of "non-linear" stratagems aimed at exploiting pre-existing structural vulnerabilities in the liberal world order whilst reducing the likelihood of reprisal or retaliation. Following the end of the Cold War, it was hoped that a more peaceable liberal world order would emerge under the benevolent rulership of American unipolarity. The liberal order sought to gradually transform acts of self-interested transactional cooperation into more enduring loyalties. Non-linear stratagems are simply a variation of this theme, albeit without the anticipated positive externalities. Operating on similar lines to realist international theory, such ploys seek to further the dual objectives of self-interest and state survival in an anarchic global system. This report provides a general theoretical examination of such emerging stratagems, using recent Iranian cyber activities to support the arguments made. To that end, we offer a deeper analysis of the findings partially presented in our recent ARTICLE 19 studies on Iran's National Internet (published in 2016) as well as a forthcoming publication on Soft War and the Iranian Cyber Army.

Section 1 – Introduction

Recent research (Pablo and Zeitzoff 2014) on emerging platforms in communications technology (Roldán 2013) has explored the ways in which non-democratic regimes (Taubman 2002) engage in concerted efforts to restrict online activity (Rød and Nils 2015) and use cyberweapons to project power internationally (Castells 2015). Computer network operations provide several clear advantages to users, offering a cost-effective and plausibly deniable weapon that allows users to control escalation in a much more measured and deliberate way than that commonly afforded by conventional forces and tactics. Cyber espionage and warfare can thus serve as a force multiplier (Sharma 2010), offering novel approaches to conflict management and presenting a way to maximize the impact of existing conventional resources and tactics. These tactics and others like them embody an evolutionary adaptation in the ways in which states interact politically, representing a set of non-linear stratagems and unconventional methods.

Non-linear stratagems are not constrained to non-kinetic engagements such as cyber warfare. Rather, this framework can be thought of as a more general reaction against the liberal world order established in the aftermath of the Cold War. This vision offered a propagation of peace and security through a virtuous cycle of self-interested cooperation, closer interconnection through advancements in information technology (for instance, a world linked together in a cooperative global village), and the resolution of disputes through the mediation of objective international organizations and regulatory bodies.

It was hoped that a more peaceable (positive-sum) world order would emerge as the tit-for-tat acts of transactional cooperation slowly shifted into more enduring loyalties: in other words, a transformation in the norms of cooperation amongst states. Non-linear stratagems are simply a variation of this theme, albeit without the anticipated positive externalities. Operating on similar lines to realist international theory, such ploys seek to further the dual objectives of self-interest and state survival in an anarchic global system.

Two recent examples shed light on the benefits offered through the embrace of such unconventional tactics. First, recent revelations of Russian intervention in the 2016 American presidential elections highlight a blurring of lines between domestic and international politics, as well as state and non-state actors. Through conjecture, one can discern the formation and development of several of the ideas that were used in this highly contentious event through the lens of the 2014 intervention in Crimea, which in some ways served as a pilot for several of the tactics employed in 2016.

Second, emerging cyber policies employed by the Islamic Republic of Iran can be seen as an embrace of similar non-linear stratagems to those used by the Russian government. Specifically, this project examines the Iranian government's domestic and internationally-oriented cyber policies through two key initiatives: the Iranian National (*Halal*) Internet and the so-called Cyber Army. These represent two sides of an emerging strategy of "soft warfare" through which the regime can take advantage of unconventional and non-kinetic resources in order to mitigate threats to regime stability (Price 2012). Though the scope and development of certain aspects of these programs remain ambiguous, they represent concerted efforts to capitalize on the benefits offered by fifth domain operations, as well as a means to use directed non-traditional and information-based campaigns to achieve policy objectives and interfere in domestic and international events without resorting to more disruptive conventional tactics. We employ the Russian example as an outline for building a general theory of non-linear action, and support this using the Iranian case study.

The remainder of the paper will be structured as follows. Section two will address the theoretical underpinnings of non-linear stratagems, examining their emergence and propagation as a function of pre-existing structural forces and novel strategies employed by revisionist states. Section three will offer substantive support for the theory outlined, using an in-depth analysis of recent Iranian cyber activities as a case study.

Section 3A examines the expansion of Iranian cyber policies, outlining the roles played by the National Internet Project and the so-called Iranian Cyber Army. Section 3B delves into the history and development of the National Internet. Section 3C deals with recent challenges to the implementation of the National Internet, and offers a potential roadmap of the future trajectory of censorship in Iran. In connection to this potential path, Section 3D offers insights into the so-called Iranian Cyber Army, and the role such an entity can play as both a domestic censor and a plausibly deniable international actor. Section 4 concludes, offering five key insights on non-linear stratagems and the future of international politics.

Section 2 – Towards a Non-linear Strategy of Conflict

Can the Iranian regime's vigorous embrace of cyber operations and Internet connectivity be conceptualized within a larger geopolitical framework? Compared to most oil-rich countries in the Middle East, Iran has a diversified economy, with a burgeoning technological and industrial sector (Spivack 2016) that has provided some protection against the symptoms of Dutch disease (Press TV 2015). A by-product of such diversification can be seen in the need to reconcile security concerns with economic growth. Contradictions between the regime's economic and religious goals have driven often-opposing policies focused simultaneously on infrastructural expansion and content suppression. This duality may be responsible for the development of practices and "soft war" tactics that have sought to seek a middle ground between the at-times opposing motivations within different factions of the Islamic Republic.

It can be argued that cyber operations of this nature can be classified as part of the soft war doctrine and incorporated into a new strategic narrative that has arisen in the post-9/11 security landscape. Soft war tactics might be seen as a subset of an emerging train of thought in international security, one that is quite similar to the so-called "non-linear" warfare that has been pivotal in Russian foreign policy in the new millennium (Pomerantsev 2014). Coined by Vladislav Surkov (a close associate of Vladimir Putin) in a short story published a few days prior to the annexation of Crimea (Ibid), non-linear war blurs several of the previously sacrosanct axioms of realist international theory. At the core of this strategy lies a reliance on deniability, using opaque means and obfuscation to prevent serious backlash and thwart the formation of a unified response by one's adversaries (The Economist 2014). Soft war tactics (of which Iran's burgeoning cyber policies can be deemed a subset) fit well into this category, and may mark the advent of an entirely novel approach to the strategy of conflict in international relations.

Surkov defines non-linear war as a novel form of conflict representing a clash of all against all. This, however, does not typify a theoretical innovation: it merely represents the pursuit of self-interest under the ordering principle of anarchy. In other words, we might view this conceptualization of non-linear warfare as a condition of risk and uncertainty emerging from a multipolar world order. In contrast to Surkov's paradigm, we offer the concept of non-linear stratagems.[1] These refer to a more general reaction against the liberal world order by those state that lack the means to confront the existing hegemon using "hard" power.

Non-linear stratagems consist of a wide variety of tactics aimed at subverting existing rules, institutions, and norms whilst retaining some degree of plausible deniability and ambiguity. Generally, they represent a blurring of distinctions between domestic and international politics, relying on the exploitation of all available structural vulnerabilities (domestic political problems/factions, institutional cleavages, special interest groups or lobbies, etc.). Increasingly, such maneuvers have taken advantage of the fifth domain (cyberspace) for information-based policies such as hacking, leaking, and spreading disinformation. More aggressive tactics such as the targeting of core infrastructural utilities (for example electricity, gas, communications, etc.) via non-kinetic operations may also be attempted. Using a combination of discrepant individuals, groups, organizations, and states, the revisionist power takes advantage of all available mutual interests and areas of cooperation in order to advance its own agenda. Linked to Schelling's paradox of weakness (Lindell and Persson 1986), an opponent's relative strength (and resulting disproportionate investment in an outcome) may be exploited to the advantage of the party with weaker or less developed interests. In other words, power asymmetries could be exploited as a vulnerability if the adversary knows that the established power stands to lose more.

What may be dubbed a combination of "non-linear" stratagems serves as an adaptive updating of existing norms, using flexibility and ambiguity to achieve a state's goals in the international sphere. Under this paradigm, the role of anarchy[2] is expanded, blurring the line between the realm of domestic and international politics. Seeping from the "third image" (which

1 We specifically use the term *stratagem* as opposed to *strategy* to emphasize the use of unconventional methods and artful schemes for the sake of achieving domestic and international political objectives. Both words stem from the Greek "*strategos*" (referring to the tactical rank of general), but stratagem derives from the old French *stratageme*, which places an emphasis on the use of unconventional and novel plans of action.

2 As defined in international relations theory, namely, a lack of a coercive sovereign that can influence states, establish rule of law, or resolve disputes. See: Waltz (1979) and Milner (1991) for a more in-depth analysis of anarchy in international relations.

traditionally defines interactions between nation-states) into the second image (the realm of the state, along with its domestic sub-components), the new paradigm assigns some of the features usually reserved exclusively for states (self-interest, utility-maximization, and an overarching desire for survival) to the domestic constituents that reside within states (Waltz 1959). Accordingly, actors within states are now assigned a greater degree of freedom with which to interact with state and non-state actors. A revisionist actor can thus leverage the supranational influence and domain of large corporations, interest groups, and non-state actors in order to get away with actions that would be against the desires of the country that houses said non-state entities. For example, a sanctioned country may leverage their economic association with multinational corporations within the boundaries of the sanctioning country in order to indirectly lobby for the reduction or removal of punitive measures. Thus, the corporation, acting in its self-interest, may be incentivized to lobby within the sanctioning country in order to prevent the implementation of potentially deleterious economic hurdles. The same bargain may be reached with other intrastate actors on non-economic issues.

At the base of this assumption is a rather uncontroversial concept central to public choice theory: smaller groups with well-defined interests and goals will more readily overcome issues of collective action, because they will be able to prevent free-riding and organize cohesion more efficiently than larger groups with more diffuse interests (Olson 2009). Ideally, both sides would benefit: the aggressor would be able to leverage expected loss of profit to gain the support of actors within the aggrieved state. Such actors are better positioned to lobby for their interests, either pushing for policies that preserve the status quo, or even using the conflict as an opportunity for rent-seeking.[3] Non-linear stratagem seeks to take advantage of increased autonomy among (assumedly self-interested) intrastate organizations to tailor actions in such a way that the risk of reprisal of retaliation is mitigated by the presence of a coalition of vested interests that would be harmed if the aggressor were punished. If this can't be achieved, non-linear stratagem would seek to conceal aggressive actions in such a way that culpability could not easily be traced back to the initiator.

The non-linear paradigm relies on the assumption that intrastate actors will be willing to use their collective action advantage to lobby for their interests, favoring stability and economic gains over traditional geopolitical alliances. Alternatively, conflicts may be managed to disguise culpability whilst focusing damage to a well-defined and limited target. This would reduce the likelihood of costly retaliation brought about by collateral damage. Taking such considerations into account, these tools or weapons could offer their wielder a significantly broader scope of action, legitimizing use in a far wider variety of circumstances than would normally be appropriate for conventional arms. Soft War doctrine falls within the scope of such a compendium of strategies.

The impetus for an evolution of the norms of international interaction can be linked to changes to the distribution of global power following the end of the Cold War. The fall of the Soviet Union created a vacuum that was replaced by a seemingly stable unipolar world order (Wohlforth 1999). However, the 9/11 attacks showed that the asymmetric power distribution was an insufficient deterrent: non-state actors could still inflict damage on a superpower through the use of unconventional tactics, without necessarily being deterred by the vast imbalance of power (Price 2014).[4] Non-linear stratagem can be seen as an update to the logic of strategic conflict that has largely shaped our understanding of international crises over the past half-century. Building on strategic restraint, power projection, and signaling resolve, the bipolar distribution of power gave way to a strategy of conflict in which the *threat* of the use of force was the fulcrum on which international crises were managed (Schelling 1960). Actual use of force was tantamount to a policy failure, because actors were unable to achieve their goals without resorting to destructive utility-decreasing force.[5] Following the destructiveness of the Second World War and taking into account the increasingly devastating nature of nuclear weapons,[6] strategic restraint created a powerful narrative for actors in the international sphere. Non-linear stratagem marks an evolution of the accepted norms of conduct as an

3 Collusion of this kind would lend itself to rent seeking, given that fact that intrastate actors would be taking advantage of the political situation to increase their share of extracted wealth without necessarily contributing to productivity.

4 See Price (2014) for a thoughtful assessment of the role of asymmetric actors in international relations.

5 This claim operates under the assumption that wars and other violent conflicts are ex-post inefficient, meaning that the share of the good to be gained in the contest is irretrievably decreased for all concerned parties once an actor has recourse to violence.

6 As well as the redefinition of nuclear arms as an acceptable strategic deterrent but an illegitimate tactical weapon.

adaptation to the blurring of distinctions between the domestic and international, offensive and defensive, and kinetic and non-kinetic. Given this shift, cyber operations fit within a larger arsenal of policies that are less strongly bound by the traditional logic that drove deterrence during the Cold War.

It is important to note that this attempt at theoretical modernization does not represent a hard-set collection of procedures and protocols. The emergence of new approaches in international relations has at times led to overgeneralizing the scope of emerging threats, viewing what amounts to an updating of strategic mindsets as the adoption of a new canon of practice. It could be argued that such an overreaction applied to the so-called "Gerasimov doctrine" of hybrid warfare (Jonsson and Seely 2015), which reported to have been responsible for Russia's successes in the Donbas region during the 2014 Crimean conflict (Jones 2014). Instead of viewing the doctrine as a fundamentally new approach to the conduct of warfare (the so-called "hybrid" model), the operations in Crimea should be viewed within the larger context of Russian military strategy. As noted in Roger McDermott's insightful critique, "Moscow shaped its operations in Ukraine not on the basis of any presumed 'model', but upon careful analysis of the operational environment. The operations reflected political constraints and restraints from the leadership in Moscow" (McDermott 2016). Similarly, the adoption of non-linear strategies and cyber operations represents a response to the restrictions faced by the Iranian regime in its operational environment. Non-linear strategies and soft war policies can best be understood as an evolutionary adaptation to pre-existing parametric constraints. Iran is not the first or only nation to consider such a shift.

The use of cyber operations during the Crimean conflict (namely, the use of targeted malware, spear phishing operations, disinformation, disruption of Internet access, and the reframing of the media narrative) represented the most comprehensive application of non-linear tactics. But such innovations did not rise out of the ether: instead, they represented an adoption of existing paradigms to fit the realities of 21st century conflict. Nor do they deviate from the traditional realist framework. Anarchy as an ordering principle is updated to apply to non-state actors, given that a globalized economy weakens domestic actors' dependence on the state. Due to the presence of alternative markets and the threat of chain ganging from increased economic interconnection, the state's leverage over internal actors is decreased and the influence of geopolitical alliances weakened. This creates space for leveraging the preferences of an adversary's domestic constituents against its overarching interests. Thus, BRIC economies such as India and China were mollified into a position of complacence with respect to Russian intervention in the Crimea, a strategic silence that received the Kremlin's gratitude (Pomerantsev 2014).

An example of this can be seen in the recruitment of ICA activists. Though evidence on recruiting practices remains anecdotal, it appears that a combination of three factors contributes to the conscription of new elements to the ICA. First, the group appeals to young and technically proficient youth who are interested in the act of hacking as a challenge in itself. Second, involvement in the ICA provides religiously motivated youth with an unofficially sanctioned channel to contribute to the preservation of moral and religious standards in domestic society. Third, involvement may represent a function of financial enticement, as evidenced in the growth of technical education in major Iranian universities and compounded by the highly transferable nature of the skills gained through participation. Whether academically, morally, or religiously motivated, these factors may present some insights into the recruitment practices of the ICA.[7] The nature and motivation of ICA actors also works towards the diffusion of boundaries between domestic and international politics, a frontier that was a key demarcation in classical international relations theory. Geopolitics ceases to become a zero-sum conflict exclusively among states, expanding downwards to include domestic and non-state actors.

Widening the definition of anarchy introduces new actors to international relations. To quote Surkov, "In the primitive wars of the 19th and 20th centuries it was common for just two sides to fight. Two countries, two blocks of allies. Now four coalitions collided. Not two against two, or three against one. All against all" (Edinger 2015). Anonymity and plausible deniability become

7 Following the Stuxnet attack in 2009, Iranian officials called for the support of tech savvy groups to help defend their country against the 'enemy.' The nationalist sentiment provoked by the Iranian officials appealed to certain educated Iranians who cared about their perceived national sovereignty. In addition to political and ideologically motivated members who joined the cyber campaign, we encountered another group in our previous study for ARTICLE 19, which was coerced to join in exchange for a pardon of previous criminal hacking activities.

assets, favoring creative tactics and encouraging more aggressive campaigns. In this context, cyber weapons provide actors with a useful policy tool because they can be used with a higher degree of impunity and to greater benefit than conventional weapons and methods. Furthermore, the diffusion of actors creates a grey area where the accepted conventions of deterrence and compellence are weakened. This thinking diverges from the mindset associated with conventional or nuclear forces because the threat of the use of force is no longer sufficient motivation for ensuring restraint. Cyber weapons offer the user anonymity and tend to have a lower overall impact, which means that there are fewer taboos associated with their use. Anonymity lends itself to the implementation of increasingly creative offensive strategies. In this sense, cyber operations provide a perfect medium for carrying out intentions in the updated security landscape. Such intentions need not be malicious, given that the newly-afforded ambiguity in state affairs can create new avenues for tacit cooperation and coordination. What is certain is a growth in the degrees of freedom afforded to the conduct of international affairs.

Further justification for the use of soft war tactics can be linked to a fear of intervention by Western regimes. This is a common theme among the practices of the three major adopters of non-linear strategies (Russia, China, and Iran), and represents a defensive countermeasure against perceived impositions on national sovereignty. The Westphalian norm of sovereignty is highly vaulted as a staple of realist international relations theory: any perceived threat against the sanctity of government action within independent national borders is treated with great suspicion and care. “Instead of an overt military invasion, the first volleys of a US attack come from the installment of a political opposition through state propaganda (e.g. CNN, BBC), the Internet and social media, and nongovernmental organizations (NGOs). After successfully instilling political dissent, separatism, and/or social strife, the legitimate government has increasing difficulty maintaining order…Once the legitimate government is forced to use increasingly aggressive methods to maintain order, the United States gains a pretext for the imposition of economic and political sanctions, and sometimes even military sanctions such as no-fly zones, to tie the hands of the besieged governments and promote further dissent” (Bartles 2016). Non-linear stratagem may thus be seen as a direct reply to perceptions of undue influence and intervention within states’ sovereign and inviolable borders.

Given the asymmetric balance of power, potential revisionists will have no choice but to adapt to the new realities of power and practice within the international system. Non-traditional and non-linear strategic behavior is facilitated by the emergence of new technological platforms providing non-kinetic alternatives for the expression of force. This, in combination with new opportunities for leveraging intrastate actors, provides a powerful arsenal of new strategies for the mitigation, management, and resolution of conflicts. The old paradigms continue to function, albeit within a slightly updated context using the tools and resources of the technological revolution. With this new strategic context in mind, we will now attempt to assess its potential applications in the Iranian regime’s methods and practices in the fifth domain.

Section 3 – Case Study: Iranian Cyber Operations

The development of Iranian cyber initiatives reflects the sheer scope of infrastructural development undertaken by Iranian authorities in line with the Fifth and Sixth Development Plans (The Fifth Development Plan 2011). Rapid growth of Internet-based projects has produced two implications. First, new research on the surge of development and investment in cyber capabilities (Anderson and Guarnieri 2016) has brought into focus the recent proliferation of hacks, targeted attacks, and monitoring activities by what appears to be a dedicated offensive unit focused exclusively on computer-based operations. The self-described Cyber Army has been suspected of taking on such a role, though the extent to which the group has benefitted from explicit government backing and support remains open to debate and interpretation. Though the group has at times benefited from the tacit approval of the Iranian government (Kamdar 2011), there remains a considerable degree of uncertainty with respect to the extent to which the group can be considered a dedicated subsidiary of the armed forces as opposed to a symbolic public relations asset. Indeed, the regime has recently practiced a policy of reticence with respect to the existence and mandate of the Cyber Army, leading to questions regarding the organization's role as a tool for influence (BBC Persian 2011).

Attempts to expand Internet access may have yielded unexpected positive externalities domestically. The ambitious nationalization project requires significant infrastructural development and promises to expand Internet connectivity to the farthest corners of Iranian territory. Before closing the net, the Iranian government will have to widen it, offering a window through which online literacy, expression, and security could be encouraged and cultivated. Ironically, the second implication may clash with the goals of the first. Internet access is now spreading to the periphery, with rural villages and distant centers joining the online communications grid. At the same time, the speed of access and coverage is improving in major hubs and urban centers. What opportunities does such an implication offer to activists, entrepreneurs, and citizens? Will it be possible to capitalize on the positive externalities that this endeavor is generating? The amplified reliance on information-based tactics may thus create a transitory period of vulnerability during which democratic norms and avenues of free expression are cultivated, despite efforts to the contrary.

The development of Iran's online capabilities may thus potentially generate unexpected externalities that affect the viability of the regime's censorship and monitoring goals in the short term. Infrastructural development is a necessary condition for the optimal deployment of fifth-domain soft war strategies. On the other hand, such growth might also bring about an expansion of the online franchise domestically. The scope of the regime's online ambitions, its strategic context, and the extent to which the two initiatives create a conflict of interests will be examined in this paper. With respect to the first and second goals, the regime's dedication to the use of "soft" policies may represent a shift towards a more covert approach to regional operations for the sake of plausible deniability. Internet-based tactics can thus be considered a subset of what might be dubbed a "non-linear" stratagem of conflict, which places greater focus on domestic actors, non-kinetic operations, information, and media relations. We argue that non-linear strategies have gained prominence in the post-9/11 geopolitical landscape, and will use Iranian cyber policies to illustrate this point.

Our preliminary research on this issue has used qualitative data, interviews, and process tracing methods to assess and gauge the progress made in implementing various soft war initiatives. Our findings testify to the concerted efforts and general policies set by the Iranian authorities, in line with the goals set in the Fifth and Sixth Development Plans.[8]

The Iranian government has devoted a considerable amount of resources in order to become a leading regional technological actor. Though development of the National Internet has fallen behind schedule, the regime has had notable successes in expanding Internet access to rural villages and increasing Internet speeds in urban centers. This has opened a window through which online literacy, security, and expression could be encouraged and cultivated.

8 The Social, Economic and Cultural Development Plans are 5-year plans, part of "Vision 2025," a strategy for long-term sustainable growth prepared by the Executive office and presented to the Majlis for adoption into law. General Policies of the Fifth Development Plan is designed to guide government policy between 2011 and 2016 and has 45 points and includes the following articles: cultural affairs; scientific and technical affairs; social affairs, economic affairs and politics; defense; and security affairs. The text of each plan is declared by the Supreme Leader to the president, and is sent simultaneously to the Majlis, the Judiciary, and the President of the Expediency Council.

Section 3A – Defensive or Offensive Cyber Strategies?

The proliferation of Internet access across the globe has had a profound impact on the freedom of information and communication. As a result, some states have engaged in concerted efforts to restrict and censor online activity, thereby limiting the potential for collective action through this medium. Parallel to this, states have increasingly begun to appreciate the value of information-based campaigns, especially given the benefits they offer with respect to flexibility of response and anonymity.

In line with the goals set in the Fifth and the Sixth Development Plans, the Iranian regime has taken concerted steps to become a leading technological actor in the Middle East. These steps, however, have taken place in conjunction with a series of policies whose objective is the restriction and control of access to the Internet. The National Internet project represents one of the regime's most ambitious undertakings, aiming to restrict and eventually quarantine Internet access to domestically generated or approved sources hosted on Iranian servers. As a defensive strategy, the goal of the National Internet is to block access to sources and resources that could potentially be used to weaken the regime's domestic control. Access to new communications platforms can ease problems of collective action, rapidly spread new ideas and connect a large portion of the domestic population.

These emerging features can pose threats to the regime's hold on power, as well as create new opportunities for dissidence and protest that may be initiated or organized outside the nation. Unfettered access to the Internet can allow Iranian citizens to view and share content that may be disapproved by state censors on grounds of morality or religious dogma. By restricting access to internationally generated or hosted websites and producing domestically made substitute services and content, the regime has been able to use the National Internet project as a defensive strategy to protect itself from developing domestic threats.

Iran has also diverted significant resources to the soft war campaign as a means of complementing its defensive cybersecurity policy with an offensive element. In this respect, the self-proclaimed Iranian Cyber Army (ICA) serves two goals. First, the ICA provides monitoring and regulatory services to protect the development of defensive Internet capabilities and limit potentially harmful citizen activity on the web, acting similarly to IRGC plainclothes forces in its function as an arm of the domestic enforcement infrastructure on the web (though without official sanction from the government). Online filtering and monitoring can serve as a cost-effective way to curb online activism and deter future protestors.[9] Filtering and blocking differ on the scale of censorship attempted, with the former referring to the removal of access to specific websites or resources, and the latter denoting a larger-scale restriction of Internet connectivity.[10] Second, the ICA has made attempts to behave as a regional and international actor in matters relating to cyber power projection and warfare. However, the extent to which this latter purpose has been developed remains unclear.

Such ambiguity is to some extent intentional: the regime gains significant freedom of action in online operations by maintaining plausible deniability with respect to its connection to the ICA. To date, there have been no attempts to recognize the ICA as an affiliate of the Iranian government. Recent attempts to suppress official ties to the organization and efforts to rebrand the Cyber Army as a non-governmental initiative provide tentative support for this conjecture. The IRGC has taken concrete steps to disassociate itself from the ICA, labeling the group "a popular and spontaneous grassroots movement" (Nasim Online 2016). This allows the group to serve as a means of perpetuating social fear domestically whilst retaining freedom to act in foreign-related matters without implicating official government bodies.

A series of reports released by the activist group "Iranian Anonymous" highlight the economies afforded by investments in soft war initiatives. In a publication titled "Operational deployment plan of the Information

9 After the 2009 Green Movement, Iranian officials learned that the Internet served as a vital means of communication and mobilization for opposition forces.

10 More technical details are available at: https://tools.ietf.org/html/rfc7754

Security Management of the IRGC," a detailed breakdown of Iranian cyber operations was published, with the group claiming that offensive and defensive cyber operations range between $300 and $50,000 USD.[11] Such projections are in stark contrast to the cost of conventional military platforms, which typically range in the millions or billions of dollars. Investments in cyber capabilities can thus be seen to offer three main advantages: granting users plausible deniability, providing economic efficiencies, and serving as a force-multiplier when applied in combination with existing military infrastructure. Although the veracity of reports released by Iranian Anonymous cannot be verified, the figures cited align closely with independent assessments of the costs of cyber operations. An investment in fifth-domain capabilities aligns with the shift towards a non-linear approach to international affairs, a notion that will be advanced later in this report.

Section 3B – The Iranian National Internet

Iran's efforts in expanding the scope and magnitude of its Internet-based capabilities have not occurred in a vacuum. Indeed, a shift towards the use of cyber strategies has been seen in several other states. Recent literature on the Chinese government's efforts at filtering content and restricting access to the web (Feng and Guo 2013) has shed light on several key questions related to censorship schemes, assessing the extent to which certain governments censor and filter online content (Xu, Mao, and Halderman 2011), how filtering tactics can focus on limiting collective action and mass movements (King, Pan, and Roberts 2013), the extent to which dedicated censorship platforms actually limit free access to information in restricted societies (Taneja and Wu 2014), and how citizens in such settings have responded to and in certain cases circumvented constraints to access (Yang and Liu 2014). Several research projects have shed light on the scope and successes of Iranian censorship of the Internet (Aryan, Aryan, and Halderman 2013), tracing the evolution of content restriction practices from physical sources to virtual ones (Bitso, Fourie, and Bothma 2013), and examining the efficiency with which reducing Internet speeds and connectivity can suppress free expression and the dissemination of ideas online (Anderson 2013).

The Iranian National Internet Project presents a stark example of such a trend. We argue that the development of a nationalized Internet service isolated from the global web represents the Iranian government's defensive strategy in dealing with domestic threats. Through a policy of content restriction, blocking, and substitution (wherein government-approved domestic substitutes that meet the regime's moral and religious restrictions are offered as stand-ins for foreign-based websites and resources deemed inappropriate by state censorship authorities), the regime has attempted to curb expression and access to information. Such tactics are rumored to have been complemented by an unofficial enforcing body known as the Cyber Army, which polices online behavior and provides an offensive arm within the nation's information infrastructure. The policies are complementary, highlighting the link between Iran's censorship policies and the growing influence of the country's intelligence and security communities in online activities following the Green Movement of 2009.

As noted in our earlier report on the National Internet (commissioned and published by the human rights organization ARTICLE 19), the implementation of the National Internet initiative was planned in three stages. The first would implement filtering and censorship procedures to sanitize online content and remove offensive or foreign content. The second phase would involve the relocation of all Iranian websites to domestic hosts. The final phase would involve the local management of all online affairs by regime affiliates. Given the ambitious scope of the plan, several major deviations and delays have already been noted, though the regime has touted the fact that nearly 40% of content accessed by Iranian Internet users is now domestically hosted (Article 19 2016).

The discrepancies and delays mentioned above have created a unique situation in which the rate of expansion of Internet access has outstripped the regime's censoring and content replacement abilities. While urban centers are granted faster bandwidth and Internet penetration spreads to the periphery, the herculean task of blocking foreign websites and content remains a significant challenge. This, in conjunction with the proliferation of Farsi-language content and heightened online awareness on the part of the Iranian

11 The group "Iranian Anonymous claims that the cost of cyber weapons is significantly cheaper than the production cost of any modern conventional arms. Such tools and weapons include ideologically and strategically motivated content creation, defacing and spear phishing campaigns aimed at opponents' official websites, stealing sensitive information, etc. For further details, see https://goo.gl/Q9lOAb

population, has ironically created a more technologically conversant population that is increasingly savvy of new loopholes and outlets to evade the pervasive reach of the authorities.

Economic pressures may also bear effect on the regime's ultimate goal of creating a hermetically sealed domestic Internet. Herein one may note a slight contradiction between two of the regime's stated goals. On the one hand, exercising control over content and communication on the web remains a central tenet directly related to the regime's religious and ethical mandates. On the other hand, the post-sanctions environment has opened several opportunities for the expansion of the burgeoning technology sector in Iran. According to World Bank estimate, a one percent increase in bandwidth penetration can generate up to 1.4% increase in economic growth within low- and middle-income countries. This trend has not been lost on the regime, which has channeled significant time and resources in order to establish Iran as a technological hub in the Middle East.

In order to achieve this vision, the regime has mandated three major policies, involving the modernization of the Internet Protocol system to IPv6, deepening connectivity and Internet penetration in rural areas, and increasing bandwidth and Internet speeds nationally. According to the World Bank, roughly 39 million Iranians had access to the Internet in 2014. Ninety-two percent of citizens had access to mobile phones. According to a Mehrnews poll, 44.7% of urban households and 17.5% of rural households currently have access to the Internet, with the majority (61.5%) using mobile devices to connect to the web (45.9% reported using personal computers) (Ibid). Legislation in 2015 has called for the connection of 25,000 more villages to the Internet in the near future, with a corresponding increase in national traffic bandwidth to 4000 gbps (a near doubling of the current national traffic bandwidth of 2400 gbps, and more than 19 times higher than the current bandwidth for international traffic, 207 gbps). Indeed, the Ministry of Communications has expressed a desire to increase national bandwidth by 80% for every 20% increase in the international bandwidth (Ibid). The culmination of this sizeable infrastructural investment is the planned expansion of Internet access to all villages with more than 20 households (accounting for some 36,000 villages) by June 2017. Around USD 80 million has been devoted to providing 8,000 villages with a high speed ADSL Internet connection, with another USD 123 million earmarked for connecting another 25,000 villages. The regime has also devoted resources to "Project Talash," which has currently laid more than 30,000 kilometers of fiber optics cable to connect the 31 provinces to 128 telecommunication stations (Ibid). The ultimate goal of this enterprise will be to triple data transmission capacity at an estimated cost of USD 70 million (Ibid).

Such infrastructural projects are producing notable results, via the provision of 20MB bandwidth, transfer of considerable financial transactions to e-payment systems, and the transfer of major government and bureaucratic services to online substitutes. All public organizations are currently linked to the national information network, and the nation possesses the second-highest bandwidth per capita in the Middle East and North Africa (Ibid). A combination of public and private sector investments has empowered the regime to expand infrastructure, develop the required technical framework, and prepare resources in order to make Iran a technological hub in the region. The prospect of foreign investment has created further opportunities for financing and implementing this vision.

This wave of infrastructural development and expansion could potentially create downstream challenges for the regime's ambitions of creating a sanitized and domestic Internet service. The implementation of the National Internet project would sever ties to the global market, crippling the burgeoning tech industry and limiting opportunities for trade and collaboration with major international players. The field of information technology is by its very nature an international one, transcending national boundaries and offering goods and services that take on a truly global scope. In addition, many of the platforms and innovations draw their edge from their ability to connect people and ideas over vast distances. By sealing off the Internet, the Iranian regime could effectively halt the growth of a very promising source of new investment and capital.

In conjunction with the aforementioned, the expansion of bandwidth and Internet coverage creates an environment in which attempts at instigating more restrictive censorship schemes are thwarted by the very infrastructural development in which the regime is engaging. By connecting more and more Iranians to the Internet, the regime creates a significant challenge for the eventual disconnection and isolation of these new Internet users. The flow of foreign capital and investments could potentially moderate the regime's attempts at nationalizing the Internet, but such an

inflow could also have a potentially perverse effect on online expression and communication in Iran. This is particularly relevant if international firms engage in the trade and transfer of dual-use technologies that could be employed to curb free expression, monitor citizens' online activity, or filter content on the web. Thus, the wave of infrastructural development creates a paradox that could potentially hinder the ultimate execution of the National Internet initiative. This, however, occurs in conjunction with a wave of foreign investment and development that could have either a positive or negative effects on free expression and communication in Iran. The contradictions between economic and religious interests remain.

The conservative religious ideology of the Islamic Republic has always been at odds with the presence of "illicit content," "cultural imperialism," and "subversive" speech (Burkhart 1998). Whilst there has been some divergence of opinion with respect to the extent to which content could be blocked or sanitized, the general reaction of regime authorities has tended to be reactive. Certain voices have suggested a pragmatic approach to dealing with the Internet (notably, seminary scholar Sheikh Ali Korani, who referred to the proliferation of access as a "reality Iran must learn to live with"), but the consensus has more closely followed views similar to those of Foreign Minister Javad Zarif, who decried the presence of offensive and "satanic" information on the web whilst advocating for the provision of "a certain level of decency" (Ibid).

Appeals to decency have at times been used as a pretext for censoring voices critical of the regime. The emergence of blogging as a major platform of communication has presented a useful case study of such filtering. Persian blogs gained prominence as an open and relatively unrestricted venue for communication in the early 2000s, filling a vacuum created by the closure of several key print publications and early news websites.[12] Interestingly, blogging habits appeared (for a time) to transcend traditional political cleavages, with key members of the Iranian government keeping personal blogs devoted to social, economic, and political matters.

12 Examples include the closure of the *Jaame'e, Salaam, Aaftab Emrooz, Sobh-e-Emrooz,* and *Asr-e-Azadegan* Newspapers. For further details, please see our forthcoming ARTICLE 19 publication on the Iranian Cyber Army.

Somewhat predictably, the sudden propagation of personal blogs was met by a wave of censorship and incarceration in the mid-2000s. Several notable bloggers were prosecuted by the regime, and at least one activist (Sattar Beheshti) was killed as an indirect result of his online activities (Beheshti died in custody in November 2012: see Kamali 2012).

Section 3C – Potential Future Trajectory of Iranian Censorship

Government policy towards the Internet has softened somewhat in the Rouhani administration, particularly towards large social media platforms like Facebook and Twitter. The thaw represents a significant change in perspective: whereas previous attempts to tame the Internet (through outright blocking and substitution) failed in curbing online expression and capturing the market, the new approach expresses a willingness to engage in new media, aiming to coopt the power of emerging networks to benefit regime interests. Perhaps following the lead of their western counterparts, many Iranian ministries and senior policymakers now maintain official Twitter accounts, using the channels to broadcast policy announcements, opinions, and reactions.

Instead of fearing social media, the incoming generation of Iranian political leaders appears to be embracing it, in doing so taking advantage of the global reach of such media in order to broadcast an alternative interpretation of regional and global affairs to an international audience. Properly used, social media can offer the regime a hitherto unexplored, cheap, and efficient public relations platform. Many in the old guard retain a robust suspicion of social networks and the Internet (in particular, the Judiciary), but the consensus appears to favor an evolutionary strategy. Responding to internal critics of their new approach, Minister of Culture Ali Jannati decried the banning of social media websites as "ridiculous," stating: "if we look back at the actions we took, we find some ridiculous decisions. For instance, bans on VCRs, VCR tapes, or even fax machines!" (Roozonline 2014).

One should be cautious to note, however, that a more media-savvy regime does not automatically imply a more open one. Indeed, a strategy of "smart filtering" has been adopted by Rouhani's Information and Communications Technology Minister, Mahmoud Vaezi. "Smart filtering means putting immoral and criminal content out of reach...the eleventh government

will implement smart filtering in order to eventually nationalize virtual networks and applications. The government has always recommended national versions of social networks" (Roozno 2015). Smart filtering capabilities are being developed with the collaboration of a "reputable" Iranian university, and the three-phase development plan appears to be making progress. "The first phase has been completed as a pilot project, and we are now running the second phase. The third phase will start six months from the completion of the second phase," Vaezi stated (Farsnews 2015). There are indications that the filtering scheme will eventually expand to mobile operators, with some USD 37 million in research agreements being allocated to 11 research universities tasked with dealing with the technical challenges faced (Tabnak 2016).

Vaezi's vision of Iran's Internet future is unambiguously nationalized: "Localized networks launched in the country were well received by the people. We hope that citizens continue to support localization as they did before." Rather ironically, the Minister has advocated for such local networks in the name of security, claiming that domestically hosted content and the localization of cyberspace affords Iranians a higher degree of protection against foreign threats.

Advanced filtering techniques have been complemented by a battery of legislation criminalizing a wide spectrum of cyber activities, as well as the heightened prominence of online moderation groups. According to a previous report by ARTICLE 19,

> In January 2010, the Computer Crime Law was introduced; a vaguely worded law banning the 'dissemination of lies' of the publication of materials considered damaging to 'public morality'. The following year, the Iranian Cyber Police (FATA), was established. Iranian Internet-repressing entities known as 'cyber squads', such as the Revolutionary Guards Cyber Defense Command (RCDC or Gerdab) were established, funded by the Iranian Revolutionary Guards Corps (IRGC). Other groups such as the so-called 'Iranian Cyber Army' also appeared in the news, notably in February 2011, when they reportedly hijacked the media outlets of Voice of America and the BBC (Article 19 2015).

This can be seen as a particularly telling indicator of one potential future trajectory of Iranian censorship and content mediation strategies. As noted earlier, the regime's phased expansion of Internet infrastructure may present a contradiction with its censorship strategies. A shift towards a more media-savvy policy of content production and management may offer an interim solution through which the regime takes advantage of the very technology it once feared. An expansion of the Internet franchise raises the median level of technological capacity among citizens. However, such an advancement occurs in conjunction with a growth in the regime's capabilities. The protection of free expression and communication on the web then becomes a function of the citizenry's efficiency in staying ahead of the regime's technical capabilities, and implementing the minimum requisite safeguards that protect anonymity and security of information online. The regime will not remain static in response to these changes: It will be up to individual citizens and interest groups to ensure that basic safeguards and best practices are adhered to.

The policies and approaches outlined above are interrelated. This new policy platform has been characterized as the "soft war" agenda (distinguishing it from "hard power" economic and military strategies conventionally employed in geopolitical struggles). In a statement addressing the demonstrations that followed the contested presidential election of 2009, Ayatollah Khamenei emphasized the importance of ideas in the emerging political ecosystem: "The most effective international weapon against our enemies and opponents is promotion" (Khamenei 2009a), later adding that "the country's priority is to fight the enemy's soft war" (Khamenei 2009b). Since 2009, the office of the Supreme Leader has made over 30 references to the soft war (Ibid).

Given its intentionally ambiguous nature, how can we conceptualize the soft war agenda? Several government platforms have provided a general sense of its scope, notably the Islamic Development Organization of Iran, part of the media arm of the Islamic Republic tasked with advancing and spreading the regime's principles and key beliefs. In a 2010 communiqué, the soft war was defined as "any kind of psychological warfare or media propaganda that targets society and induces the adversary to accept failure without resorting to open military aggression. Acts of agitation, cyberwar, and

the use of radio-television broadcasts and rumors are important tactics within the soft war agenda" (Islamic Development Organization of Iran 2010).

Similarly, Ali Mohammad Na'ini (former deputy head of the Basij militia for cultural and social affairs) elaborated on the concept, linking the soft war agenda to tactics deployed during the Islamic revolution:

> The main principle of that revolution was the soft power of the revolution, namely the ability of the leadership to arouse an entire nation… The main aim behind the soft war is to force the system to disintegrate from within in view of its values, beliefs, its main fundamental characteristics, and its identity. Any system, especially a system that is based on certain beliefs and values, owes its identity and its existence to those beliefs and values. It is based on the models and principles on which it continues its political, social and economic life…If the identity or the fundamental beliefs and values and the main model of a revolution in different social, political, cultural and economic fields are challenged by non-military means, the adherence of the society to that system would be challenged. Quite naturally, this would lead to the ineffectiveness and the invalidation of that model, it would weaken the different pillars of the society, and subsequently the system would start to disintegrate from within. Therefore, soft war aims at confronting the main blueprint and the main ideas of a political system in different fields. By making use of its soft power, namely its culture and values, its cultural and political values and its cultural products the enemy will try to win the trust of the public [in the enemy's values]. In this way, it infiltrates the different intellectual, mental and spiritual layers of the society, and it will undermine the strength and validity of that system and will sap public trust in it. Thus, it will destroy the effectiveness of a system and would give rise to instability, and that instability and lack of trust in turn will result in civil resistance" (Price 2012).

IRGC forces have largely spearheaded the soft war initiative (Tnews 2015, Basij Press 2012, Farsnews 2014), running a range of conferences and training sessions focused on spreading the mandates of this initiative across the Iranian political and military landscape (IRNA 2015). Many of these initiatives have been co-sponsored with official channels such as the Islamic Republic of Iran Broadcasting Corporation (IRIB),[13] whose Basij contingent has commented on the group's progress in establishing "seven cyber battalions consisting of media experts and specialists" since 2011 (Farsnews 2012). This figure was corroborated by Mohammad-Hussein Firuz, secretary of the IRIB Basij Cyber Battalion Conference, who noted that their seven cyber battalions were dedicated to media outreach, Islamic teaching, women's rights, and family values. Consisting of 1,200 active members, each battalion includes experts in blogging, social media, and public relations. This group complements an additional "five special workgroups responsible for supporting the battalions in monitoring, trend studies, education and planning, supply and production, security, technical issues, infrastructural development, and maintenance" (Booshehr Basij 2012).

The ICT (Information and Communication Technology) Basij Organization may be seen as a direct expression of the central tenets of the soft war paradigm. Established with the intention to "defend the country in soft wars," the organization issued a statement indicating that 8,000 Basijis were recruited to facilitate the establishment of the "clean" Internet in Iran: "Our country is under constant cyber-attacks fueled by technological advancements aimed at infiltrating and taking down websites" (ARTICLE 19 2016). Basij forces also founded the "Basij Cyber Council" in 2010 in order to recruit hackers to infiltrate networks of opposition activists. In November 2010, Hussein Hamedani, Former Commander of the Tehran IRGC, reported that 1,500 "cyber commandos" had been trained for the Basij Cyber Council under the supervision of IRGC technologists (Tabnak 2010, pririb.ir 2014).

Such initiatives are indicative of recent advancements in the IRGC's technical capabilities. Tehran's Revolutionary Guard Corps (the Mohammad Rasul-Allah Army of the Revolutionary Guards of Tehran) provided training in audio-visual programming, social networking, game design, animation, and graphic design to over 3000 recruits as a part of a specialized one-year program (Khabaronline 2015). Several other

13 Known as the official "Voice and Vision of the Islamic Republic of Iran," the IRIB is a media conglomerate with a monopoly on domestic radio and television services in the country. Although officially independent of the Iranian government, the head of the IRIB is appointed by the Supreme Leader.

projects (such as "Mozelin," "Darkoob," and "Mersad") have focused on filtering obscene content (Gerdab 2015), arresting non-compliant or subversive web-site managers,[14] countering intelligence operations by foreign nations (Gerdab 2015), and monitoring content posted on Facebook (Gerdab 2016).

Both Basij and IRGC forces practice a dual-use mandate that can thus simultaneously serve the interests of the regime's domestic filtering and international cyber-defense needs. Reports of the existence of hacking collectives date back to the early 2000s, with groups engaging in "surveying and combatting potential cyber threats and 'alleged cyber threats against national security'" (Home Office 2014).

With respect to Internet-based operations, Iran has been engaged in a concerted effort to expand Internet access whilst blocking foreign websites and limiting the use of VPNs for circumventing domestic filters. "By building filtration mechanisms into the infrastructure, the government will not only increase its control over the flow of information within Iran, but also information coming in and out" (Ibid).

Since first connecting to the World Wide Web, Iran has spent considerable resources in order to position itself as a regional leader in Internet access and cyber technology. Iran's first commercial Internet Service Provider (ISP) was established in 1993. Two years later, the non-profit Neda Rayaneh Institute (NRI), an affiliate of the municipal government of Tehran, began offering Internet access in February 1995.

Parallel to this growth, the regime has taken concerted efforts to shore up its tactical cyber capabilities, investing in the resources and manpower required to maintain a strategic presence in fifth domain operations. These efforts have targeted both domestic and international threats, replying to pressures posed by foreign powers as well the potential for internal dissent (be it fomented through popular discontent or through some form of third-party intervention). Once again, the application of online strategies provides support for the implementation of a more flexible non-linear stratagem, seeking to optimize cyber capabilities to deal with a diverse assortment of domestic and international threats.

14 For more information, please see: http://gerdab.ir/fa/print/256 and http://gerdab.ir/fa/print/334 and http://gerdab.ir/fa/print/227 and http://gerdab.ir/fa/print/157 and http://gerdab.ir/fa/print/73

Section 3D – The "Cyber Army" and its Functions

An early demonstration of the regime's willingness to limit Internet access came just six months after it was first offered to Iranian citizens: "In early August 1995, all 200 of NRI's dial-up lines were disconnected by the Telecommunications Company of Iran (TCI)" (Ibid). Filtering was made possible through the provision of bureaucratic safeguards that placed control of the web under the jurisdiction of the regime. This can be seen in the supervision of the Telecommunication Infrastructure Company (TIC) by the Ministry of Information and Communications Technology (ICT), effectively granting the regime a "monopoly over the purchase of international Internet gateways in Iran" (OpenNet Initiative 2013).

Censorship and filtering activities followed less than a year after the country gained access to the Internet. Such efforts peaked during the disputed 2009 presidential elections, during which Mehdi Karoubi and Mir-Hossein Mousavi, the comparatively moderate challengers to Mahmoud Ahmadinejad, took advantage of Internet-based resources in order to appeal to their younger and more urban support base. Karoubi and Mousavi made use of online facilities in order to offset the wide media advantage afforded to Ahmadinejad by conventional outlets. In response to the threat posed by a wide-reaching social mobilization initiative, the social media campaigns of both candidates were regularly filtered. Nearly all websites supportive of the pro-reform candidates were blocked (Hamvatan Salam 2009). In addition, attempts were made to prevent the use of messaging applications such as g-chat, leading to public outrage and protest (Google Transparency Report 2016). In some cases, Internet speeds were even throttled to 128 kbps in order to prevent mobilization through online platforms and messaging apps. The strong backlash against Mousavi and Karoubi played a notable role in the emergence of the "Green Movement," and ultimately led to widespread changes to the means through which the regime addressed the potential risk posed by the Internet (ARTICLE 19 2016).

Filtering and throttling initiatives were both strengthened in the aftermath of the Green Movement. In addition to the frequent blocking of foreign or "offensive" websites, considerable efforts were made in order to provide Farsi-language alternatives to existing websites such as the government-sponsored "National Email" service. Other attempts involved the creation of an ersatz

video sharing service comparable to YouTube (named "Apparat"), and a local version of Facebook ("Face-Name"). None of these initiatives appear to have taken off, leading to a decrease in investment and a shift towards a permit-based system of publication that threatens non-compliance with filtering and criminal prosecution.

Filtering initiatives undertaken under the National Internet plan have not slowed down under the presidency of Hassan Rouhani, under whose tenure significant progress has been made in the implementation of "smart filtering" technologies. Though hardline elements such as the Judiciary have at times questioned the current presidential administration's commitment to installing a "Halal" Internet service, it appears that much of the work done in this arena continues to follow Supreme Leader Ayatollah Khomeini's call for the instigation of an ideological soft war in the fifth domain. This implies focusing efforts on expanding the efficiency of filtering and censorship initiatives, generating substitutable content that would meet the religious standards of the regime, and at least theoretically maintaining a dual-use responsive capability that would be able to confront online challenges to the regime.

The judiciary's decision to monitor user activities and cyberspace communications marks a significant benchmark in the regime's enforcement and monitoring practices. The traditionally conservative body plays a central role in filtering and censoring content deemed to be in violation of Iranian cyber laws or else falling short of the regime's religious and ethical standards (Pajvak 2015). As of October 2015, 2,600 judges were trained to adjudicate on issues related to cyberspace, in line with the concerns of Hojjat al-Islam Hadi Sadeghi (the Judiciary's Deputy in charge of Cultural Affairs), who cited a pressing need to "bridge the legal gap and cover loopholes in the cyberspace…This situation resembles the one we encountered during the Iran-Iraq war, in which we were empty-handed in fighting Saddam and the Ba'th regime, who were armed to the teeth; while in that tough war we could stop the enemy by sacrificing ourselves physically, today we should replace those old techniques with new ones to achieve success in the cyber war" (Mehrnews 2015; ISNA 2015).

As noted in our ARTICLE 19 report (ARTICLE 19, forthcoming), the self-proclaimed Iranian Cyber Army's affiliation and patronage is intrinsically difficult to establish. The organization is not hierarchically ordered, nor does it maintain explicit links to the Iranian Army or Revolutionary Guard Corps. Great care has been taken to prevent the authentication of a direct link or relationship to existing government organizations. The resources and infrastructure required for the maintenance of such a large collective of hackers does raise questions regarding their financial backing, but thus far any evidence linking the group to a particular branch of the government has been largely circumstantial. Members of the ICA have expressed a desire to uphold and protect traditional thought and Iranian Islamic values, but such acts have been conducted through the use of proxies (young, technologically savvy information specialists who appear to have been trained in surveillance, psychological operations, and hacking). They target both domestic and international entities.

ICA proxies have traditionally had a symbiotic relationship with the general interests of the regime, structuring their domestic practices according to three aims. The first involves participating in content creation, be it in the form of domestic hosting, the development of state-sanctioned apps, or the foundation of websites providing filtered substitutes to foreign-produced content. The second line of activity involves cyber-attacks, be they aimed at foreign or domestic websites, individuals, or organizations. As noted above, a certain degree of synergy has been detected in the targeting practices of ICA proxies, but such links remain circumstantial. Cyber-attacks have traditionally followed three objectives: information extraction, surveillance, and online intimidation. Following from the aforementioned, the third goal has seen the revealing and reporting of dissident activists to law enforcement agencies within the regime, which have benefitted from ICA leaks revealing the identities and activities of social activists, bloggers and journalists.

Though lacking the explicit support of the regime, such activities have had a rather drastic chilling effect on online expression in Iran. Targeted hacks and identity leaks create an atmosphere of mistrust and suspicion. Many citizens are disincentivized from engaging online from fear of facing the extreme sanctions suffered by those who were compromised and prosecuted by the authorities. Though online vigilantes have a relatively limited policing presence on the web, the fear of exposure creates a powerful deterrent that fuels self-censorship in the name of prudence. Human rights activists and pro-reform campaigners have noticeably felt the effects of the new atmosphere of paranoia. As a result of the often-lax security provisions practiced

by such advocates, many have faced censure, imprisonment, or worse. Hackers often take advantage of glaring vulnerabilities in online security, exposing the identities of activists and divulging their practices to the authorities. Through psychological pressure and other forms of ill treatment, authorities are then able to extract key information on other activists, compromising the greater network.

As noted in Anderson and Guarnieri's (2016) recent work on Internet-based policies within the Iranian soft war agenda, the Islamic Republican government has sought to implement a responsive rejoinder to what it has deemed a concentrated policy of "continual intrusion campaigns from foreign actors that sought access to the country's nuclear facilities, economic infrastructure, military apparatus, and governmental institutions for the purpose of espionage and coercive diplomacy." Following the attacks, Iranian actors were discovered to be responsible for several campaigns aimed at sabotaging and vandalizing websites run by adversarial foreign actors and dissident movements, suggesting that investments in cyber operations have begun to take on a decentralized and domestically cultivated valence (Ibid).

Acts of online intervention appear to be directed against two main sources: dissident critics and perceived international challengers. Interestingly, the distinction between such groups appears to be blurring, as noted by Anderson and Guarnieri's assertion that "Iranian threat actors maintain a consistent set of interests and activities that blur the lines between domestic surveillance and foreign commercial espionage" (Ibid). They note that 48% of identified attacks are aimed at targets within Iran, with the remainder "distributed around the world, with a higher concentration in the United States, Sweden, Germany and Iraq – locations with large Iranian Diasporas or regional interests. Several compromised systems maintain a clear relationship to regional adversaries and foreign entities that Iran maintains an espionage interest in" (Ibid).

This would suggest that multipurpose platforms and tools have been able to successfully take advantage of vulnerabilities left by lax security standards and poor personal data safety practices. Though such vulnerabilities are often quickly addressed and strengthened, Iran-based actors have shown notable assiduity in finding and exploiting new weaknesses, often taking advantage of common psychological and behavioral weaknesses to engineer the extraction of information under guileful pretexts. In some cases, activists posed as affiliates of international organizations or human rights groups and sent victims forged presentation outlines with embedded malware (Franceschi-Bicchierai 2016). Similar forms of manipulation have been used to trick internal and external targets into accepting malware-laced emails, oftentimes using the identity of a trusted source as a cover to either install surveillance software or to gain control over the platform and message of an adversarial critic or organization.

The use of such diverse tactics, in conjunction with a creative campaign of deception, misinformation, and strategic targeting can all be seen as a part of an overarching soft war strategy aimed at making full use of non-conventional and non-linear operations. In addition, the quality of such campaigns appears to be improving, thanks to more nuanced targeting strategies and superior social engineering tactics (Anderson and Guarnieri 2016).

Iran's presence in cyberspace has played a central role in the nation's domestic and foreign policy strategies, pooling resources in order to efficiently address domestic threats to the sanctity of the regime whilst simultaneously providing an offensive toolkit aimed at weakening and balancing external threats. With regards to the latter, Anderson and Guarnieri note the use of politically charged controversies as a pretext for compromising human rights organizations and international media outlets (as seen in the activities of the "Infy" group), in certain cases using actual stories related to political prisoners, political censorship, and acts of repression as a pretext for proliferating malware embedded in Word, PowerPoint, or PDF documents (Ibid).

Recent attacks such as the hacker Sima Group's February 2016 targeting of Iran-focused activists using fabricated messages impersonating the Emergencies Director of Human Rights Watch display the increasing intricacy and competence of directed attacks. Providing legitimate secondary links and referencing an existing report produced by Human Rights Watch, the attackers "demonstrated stronger English-language proficiency than past intrusion sets and a deeper investment in background research prior to the attempt. The actors appropriated a real identity that would be expected to professionally interact with the subject, then offered validation through links to a biography and social media profile, both of which were also infected with

malware. The bait documents contained a real article relevant to their interests and topic referenced, and the message attempted to address to how it aligned with their professional research or field of employment" (Ibid).

The attacks mark a shift from earlier tactics, which relied on the transmission of a high volume of generic malware in the hopes that the victim would eventually click on one of the traps. The use of more nuanced ploys such as the studied impersonation of a known entity, the tailoring of messages for very specific targets, and the use of elements of legitimate sources and websites suggests a heightened degree of premeditation. It might even be taken as an indication that the attackers are engaging in the long-term surveillance and observation of their targets, tracking their habits and creating messages that correspond to their professional activities. With respect to the targeting of human rights and women's rights activists, the newfound nuance and personalization of spear phishing attempts "supports the theory that this campaign is, to the best of our knowledge, dedicated to the surveillance of members of Iranian civil society and diaspora" (Ibid).

As with all attacks attributed to the Cyber Army, official government sponsorship of hacks and surveillance activities cannot be established. However, the timing and frequency of incidents appears to provide at least circumstantial evidence supporting the existence of some level of coordination between activist groups and the regime. Certain attacks appear to follow as responses to political events affecting Iranian interests. And as with most of Iran's recent efforts in bolstering soft war tactics, the campaigns rely on dual-use resources that combine offensive and defensive capabilities in a way that allows the regime to project power whilst protecting key assets from external attack.[15]

15 This was most recently seen in the discovery of industrial malware in the regulatory software of two key petrochemical plants, following a fire at the Abu Ali Sina refinery complex in July. Though the National Cyberspace Council has stated that the fire was likely the result of poor health and safety standards, the organization remains alert to the threat of cyber-attacks. For more details, see: http://www.reuters.com/article/us-iran-security-cyber-idUSKCN1120E9

Section 4 – Conclusion

The analysis of non-linear stratagems offered in this paper represents reaction against the existing liberal world order by those states who lack the capacity to confront the established hegemon using "raw" power. The concepts explored here represent an updated and relaxed variation of realist doctrine, highlighting the importance of plausible deniability, information technology, and intrastate actors. Five key insights may be derived from the analysis of non-linear stratagems offered in this report.

1. Emerging technological innovations and platforms offer state and non-state actors a greater degree of flexibility with which to pursue their objectives. Plausible deniability and ambiguity lower the potential costs of intervention by reducing the risk of successful attribution and retaliation. These tools are often multi-purpose, granting regimes the latitude to conduct campaigns against domestic and foreign adversaries using the same hacking, blocking, and phishing toolkits.
2. Information platforms can be used to blur the boundary between domestic and international affairs. Social networks can be leveraged for or against the interests of the regime, offering potential benefits for free expression and communication as well as new risks to those rights, should they be applied by those who seek to capture or limit the communication of potentially subversive ideas. In the case of Iran, an increasingly universal access to information is now a political reality: instead of seeking to pursue traditional policies of censorship and content suppression, the regime has instead adapted to the new media environment, capitalizing on existing platforms in order to generate content and take control of the narrative. In the case of Russia, strategic hacks and leaks have been used to influence the outcome of the 2016 American presidential elections in favor of a friendly candidate.
3. Cyber operations can be used as a force multiplier to complement pre-existing military and diplomatic infrastructure and resources. Online campaigns offer a greater degree of protection than costly kinetic involvements, offering actors with a more nuanced avenue for action in such a way that provides superior conflict management and escalation prevention. This represents an evolutionary adaptation to the emergence of perceived vulnerabilities in the fifth domain. Psychological operations and intelligence have been central to warfare for millennia: non-linear stratagems simply seek to update these assets using 21st century innovations. These capabilities may even allow revisionist regimes to simultaneously reintegrate into the global economy while furtively continuing questionable domestic and regional agendas without a severe risk of blowback or exposure.
4. Emerging non-linear stratagems blur the boundaries between actors and bystanders, thus allowing for greater freedom of independent action by non-state and intrastate actors.
5. Distinctions between offensive and defensive capabilities are rendered increasingly opaque. Dual-use technologies allow actors to make full use of available resources in order to achieve desirable outcomes in conflicts. Cyber operations in particular lend themselves to such flexibility because there are no well-defined rules of engagement or enforcement mechanisms. Such tactics are still in their infancy and are constantly evolving with the times. As with any emerging strategy, any vulnerability created today will be met with advances in security measures tomorrow. The rate of change has accelerated, but the mechanism of change remains somewhat constant.

These concepts shed light on the emerging risks and opportunities presented by non-linear stratagems. Recent developments in Iranian and Russian behavior serve as an important lens for understanding these innovations and their implications, highlighting the complexity and ambiguity of the issues at play. Through the soft war paradigm, we are afforded a glimpse into what the future of international affairs

may come to look like. Similarly, non-linear stratagems offer an attractive way through which states may use existing vulnerabilities in the international system to their advantage. This future is one in which emerging and revisionist powers such as China, Russia, and Iran can leverage unconventional tactics, emerging technologies, and the new realities of an increasingly interconnected and globalized world in order to simultaneously achieve domestic and foreign policy goals. The blurring of territorial lines, economic codependence, and a technological revolution in information have created new avenues in which states can hedge against one another for the sake of survival and security.

Instead of engaging in acts of traditional military or diplomatic balancing against the existing global hegemon (the United States), countries can now take advantage of subtler tactics that exploit the vulnerabilities exposed within the very liberal world order the hegemon initially established. Instead of changing the rules of international engagement, non-linear stratagems seek to bend and creatively interpret existing rules and norms in order to seek strategic advantages and benefits. Incidents like the Stuxnet attack and the unconventional Russian intervention in Crimea have opened Pandora's box, exposing an entire set of hitherto-unexplored strategic possibilities, most of which can be seen as creative responses against the overwhelming power imbalance between the United States and the "rest." Now that a precedent has been set, states may feel increasingly emboldened to achieve their goals through similarly nuanced measures, responding to the unipolar world order through a set of policies that seek to capitalize on its emerging idiosyncrasies. It is in the best interest of the hegemon to attempt to neutralize this precedent instead of retaliating in kind: such a reaction would only serve to further legitimize the non-linear stratagems employed by revisionist actors in the pursuit of their goals. Just as in nature, states will do all they can to survive: we are witnessing nothing short of Darwinian adaptation.

Bibliography

"The Assumption of Anarchy in International Relations Theory: A Critique." *Review of International Studies* 17.1: 67-85. Web.

"A Centre for Fighting Social and Cultural Corruption." 2015. *Gerdab*. January 31. Accessed March 1, 2016. http://gerdab.ir/fa/print/13567

"After the Green Movement: Internet Controls in Iran, 2009-2012." 2013. *OpenNet Initiative*.

"Basij Trains 1500 Cyber Commandos." 2010. *Tabnak*. November 21. Accessed March 1, 2016. https://goo.gl/zdlI6X and "Cyber Armies Mobilized in the National Media." 2014. pririb.ir. November 29. Accessed March 1, 2016. http://www.pririb.ir/persian/ModulesPage.aspx?modulename=news2&action=viewtext&news=42569 and "Open Letter Released by Student Basij Office of Alborz Universities." 2015. *Basijnews.* October 13. Accessed March 1, 2016. http://goo.gl/CNTbOZ

"Communication Minister Opposes Filtering." 2015. *Roozno*. February 3. Accessed March 1, 2016 http://goo.gl/bK1P5X

"Computer Crimes in Iran – Risky Online Behavior." 2015. *ARTICLE 19.*

"Country Information and Guidance, Iran: Journalists and Bloggers." 2014. *Home Office*. October 9. Accessed March 1, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/362260/CIG_-_Iran_-_Journalists_and_Bloggers_-9_October_2014.pdf.

"Cyber Criminals." 2015. *Gerdab*. September 15. Accessed March 1, 2016. http://www.gerdab.ir/fa/print/15588

"Establishment of 7 Cyber Armies in the National Media." 2012. *Farsnews*, December 24. Accessed March 1, 2016. http://www.farsnews.com/newstext.php?nn=13910926000786

"Get to Know IRGC Cyber Forces." 2015. *Khabaronline*. September 2. Accessed March 1, 2016. http://www.khabaronline.ir/detail/453114/Politics/military http://hizbullahcyber.com/content/25123

"Government Seeks Smart Filtering." 2015. *Farsnews*, February 2. Accessed March 1, 2016. http://www.farsnews.com/newstext.php?nn=13931113001048

"Iran says wary of 'Dutch Disease' once sanctions lifted." 2015. *Press TV*. March 28. Accessed September 27, 2016. http://www.presstv.com/Detail/2015/03/28/403740/Iran-says-wary-of-Dutch-Disease

"Iranian Officials Hesitant About IRGC Cyber Army." 2011. *BBC Persian*, September 6. Accessed September 27, 2016. http://www.bbc.com/persian/iran/2011/09/110906_l39_mehdi-sarami_iran_cyber_armi.shtml

"IRGC Uses All Capacity to Fight Soft War." 2015. IRNA. October 17. Accessed March 1, 2016. http://www.irna.ir/fa/News/81802788/ and "IRGC's Significant Success in Fighting Soft War." 2015. *Basijnews*. April 22. Accessed March 1, 2016. http://goo.gl/i3A8mB

"Known disruptions of traffic to Google products and services." *Google Transparency Report*. Accessed March 1, 2016. https://www.google.com/transparencyreport/traffic/disruptions/#region=IR&expand=Y2012,Y2011,Y2010,Y2009

"Launch of the Judiciary's Social Network." 2015. *Pajvak*, September 16. Accessed March 1, 2016. http://goo.gl/pUoR58

"Mobile Operators Subject to Smart Filtering." 2016. *Tabnak* February 22. Accessed March 1, 2016. http://goo.gl/AQiVPr

"National Media Cyber Armies Have More than 1200 Members." 2012. *Booshehr Basij*. December 8. Accessed March 1, 2016. http://booshehr.basij.ir/?q=node/3298

"New Details on the Spider Project." *Gerdab*. March 1. Accessed March 1, 2016. http://gerdab.ir/fa/print/13613

"New Round of Filtering in Iran." 2009. *Hamvatan Salam*. April 4. Accessed March 1, 2016. http://www.hamvatansalam.com/news128805.html; and, "Facebook Is Finally Filtered." 2009. ITNA. May 24. Accessed March 1, 2016. http://www.itna.ir/vdcc0eqs.2bqix8laa2.html

"No ICA in IRGC Organisational Chart." 2011. *Nasim Online*. September 9. Accessed March 1, 2016. http://old.nasimonline.ir/NSite/FullStory/News/?Id=268650

"Seyed al-Shohada Sepah Ready to Fight the Enemies' Soft War." 2015. *Tnews*. September 8. Accessed: March 1, 2016. http://tnews.ir/news/C0ED47835908.html and "Soft War Workshop." 2012. *Basij Press*. January 29. Accessed March 1, 2016. http://basijpress.ir/fa/news-details/4924/ and "Soft War Exhibition in Ijroud." 2014. *Farsnews*. November 6. Accessed March 1, 2016. http://www.farsnews.com/newstext.php?nn=13930815000074

"Supreme Leader Meeting with AoE Members." 2009a. *Khamenei.ir.* September 24. Accessed March 1, 2016. http://farsi.khamenei.ir/speech-content?id=8094

"Supreme Leader Meeting with Basij Members." 2009b. *Khamenei.ir.* November 25. Accessed March 1, 2016. http://farsi.khamenei.ir/news-content?id=8429

"The Judiciary Enters Chat Space." 2015. *Mehrnews,* October 15. Accessed March 1, 2016. http://goo.gl/HwnefE. See also: "Filling the Legal Gap in Cyberspace." 2015. ISNA. September 19. Accessed March 1, 2016. http://goo.gl/uitcMa

"The Prohibitions are 'Ridiculous'." 2014. *Roozonline*. March 3. Accessed: March 1, 2016. http://www.roozonline.com/persian/news/newsitem/article/-6a00ec05e3.html

"Tightening the Net: Internet Security and Censorship in Iran." 2016. *ARTICLE 19*. Part 1: The National Internet Project: 1.

"War by Any Other Name." 2014. *The Economist*. July 4. Accessed September 27, 2016. http://www.economist.com/news/europe/21606290-russia-has-effect-already-invaded-eastern-ukraine-question-how-west-will

Anderson, Collin, and Claudio Guarnieri. 2016. "Iran and the Soft War for Internet Dominance." https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf

Anderson, Collin. 2013. "Dimming the Internet: Detecting throttling as a mechanism of censorship in Iran." *arXiv preprint arXiv:1306.4361*.

Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 2013. "Internet censorship in Iran: A first look." *Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet.*

Barberá, Pablo, and Thomas Zeitzoff. 2014. "The Empirical Determinants of Social Media Adoption by World Leaders and its Political Consequences."

Bartles, Charles K. 2016. "Getting Gerasimov Right." *Military Review 96.*

Bitso, Constance Majomane Likonelo, Ina Fourie, and Theodorus Jan Daniel Bothma. 2013. "Trends in transition from classical censorship to Internet censorship: selected country overviews."

Burkhart, Grey E. 1998. "National security and the Internet in the Persian Gulf Region."

Castells, Manuel. 2015. *Networks of outrage and hope: Social movements in the Internet age*. John Wiley & Sons.

Edinger, Harald. 2015. "Russia and the Making of Post-Cold War Geopolitics." *Project Firefly.* Accessed September 27, 2016. https://project-firefly.com/node/19378

Feng, Guangchao Charles, and Steve Zhongshi Guo. 2013."Tracing the route of China's Internet censorship: An empirical study." *Telematics and Informatics*. 30.4.

Franceschi-Bicchierai, Lorenzo. 2016. "How Researchers Exposed Iranian Cyber attacks Against Hundreds of Activists." *Motherboard Vice.* August 11. Accessed September 16, 2016. https://motherboard.vice.com/read/iran-cyberattacks-against-activists
Jones, Sam. 2014. "Ukraine: Russia's new art of war." *Financial Times* August 28. Accessed: September 27, 2016. https://www.ft.com/content/ea5e82fa-2e0c-11e4-b760-00144feabdc0
Jonsson, Oscar, and Robert Seely. 2015. "Russian full-spectrum conflict: An appraisal after Ukraine." *The Journal of Slavic Military Studies* 28.1.
Kamali Dehghan, Saeed. 2012. "Iran accused of torturing blogger to death." *The Guardian*. November 8. Accessed March 1, 2016. www.theguardian.com/world/2012/nov/08/iran-accused-torturing-blogger-death
Kamdar, Nazanin. 2011. "Conflicting Postures Over the Cyber Army." *Payvand.* September 22. Accessed September 27, 2016. http://www.payvand.com/news/11/sep/1225.html
King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107.02: 326-343.
Lindell, Ulf, and Stefan Persson. "The paradox of weak state power: a research and literature overview." *Cooperation and conflict* 21, no. 2 (1986): 79-97
McDermott, Roger N. 2016. "Does Russia Have a Gerasimov Doctrine?" *Parameters* 46.1: 97.
Olson, Mancur. 2009. *The logic of collective action.* Vol. 124. Harvard University Press.
Pomerantsev, Peter. 2014. "How Putin Is Reinventing Warfare," *Foreign Policy*. May 5. Accessed November 30, 2015: http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/
Price, Monroe E. 2014. *Free expression, globalism, and the new strategic communication*. Cambridge University Press.
Price, Monroe. 2012. "Iran and the Soft war." *International Journal of Communication* 6: 19.
Rød, Espen Geelmuyden, and Nils B. Weidmann. 2015. "Empowering activists or autocrats? The Internet in authoritarian regimes." *Journal of Peace Research*. 52.3: 338-351.
Roldán, Alba Mohedano. 2013. *Political Regimes and the Use of the Internet by Social Movements*. Center for Comparative and International Studies (ETH Zurich and University of Zurich).
Schelling, Thomas C. 1960. *The strategy of conflict.* Harvard university press.
Sharma, Amit. 2010. "Cyber wars: A paradigm shift from means to ends." *Strategic Analysis* 34.1: 62-73.
Spivack, Matthew. 2016. "What to Know About Doing Business in Iran." *Harvard Business Review*. May 5. https://hbr.org/2016/05/what-to-know-about-doing-business-in-iran
Taneja, Harsh, and Angela Xiao Wu. 2014. "Does the Great Firewall really isolate the Chinese? Integrating access blockage with cultural factors to explain Web user behavior." *The Information Society* 30.5: 297-309.
Taubman, Geoffry. 2002. "Keeping Out the Internet? Non-Democratic Legitimacy and Access to the Web." *First Monday* 7.9. Accessed August 27, 2016.
The Fifth Development Plan. 2011. *Majlis Research Center*, January 20. Accessed September 27, 2016. http://rc.majlis. ir/fa/law/show/790196
Waltz, Kenneth Neal. 1959. *Man, the state, and war: A theoretical analysis.* Columbia University Press.
Waltz. 1979. A Theory of International Politics; and Milner, Helen. 1991.
Wohlforth, William. 1999. "The Stability of a Unipolar World," *International Security*: 5-41.
Xu, Xueyang, Z. Morley Mao, and J. Alex Halderman. 2011. "Internet censorship in China: Where does the filtering occur?" *International Conference on Passive and Active Network Measurement*. Springer Berlin Heidelberg.
Yang, Qinghua, and Yu Liu. 2014. "What's on the other side of the great firewall? Chinese Web users' motivations for bypassing the Internet censorship." *Computers in human behavior* 37: 249-257.