CYBER WARFARE QUICK REFERENCE

Focus on Iran

ABSTRACT

This Human-shaped / AI-conducted analysis reveals how Iran navigates the complex web of international sanctions, strategic alliances, and internal dynamics to shape its cyber espionage efforts, and is additionally a useful look into human-AI collaboration for higher-order operations.

Ian Bennett

I can be reached on LinkedIn (please connect!):
https://www.linkedin.com/in/subtropicalhorseback
or through email here:
subtropicalhorseback@gmail.com

I am based near Dallas-Fort Worth, Texas, USA.

I am seeking work as a Cyber Intelligence Analyst, and this document is intended as a portfolio piece.

CAVEAT

The following analysis is conducted by AI/LLM Google's Gemini Ultra 1.0 and OpenAI's ChatGPT4 using my analytic framework.

All information used for the analysis is their respective cached information, their own internet searches, and their inference or deduction based on that data. This is the primary reason for lack of citations: the respective models were not able to make appropriate reference to original data sources.

I make ***zero*** guarantees about the accuracy, and this document should be used only as a general introduction into the content discussed.

I will say that the underlying data *feels* accurate, and from an analytic perspective, the conclusions and insights derived from the dataset are generally reasonable and logical.

Contents

Preface

I am a professional intelligence analyst with ten years of experience working in the US Intelligence Community. I have recently transitioned my career focus to the cybersecurity industry, and as an extension, have greatly increased my willingness and interest in use of AI or LLM tools.

I see a gap in industrial knowledge, hidden in the lack of understanding – or perhaps lack of emphasis - regarding how cyber activity by various APTs, particularly those that have demonstrated state support from 'hostile' nations, are frequently an extension of those respective countries' foreign policy implementation.

Unfortunately, I lack the country-specific expertise and the time, resources, tools, etc. to study *every single country* that is known or suspected to be a source of cyber activity that threatens US, or more broadly, Western interests – whether PII for citizens, private industry IP, money, government espionage, critical infrastructure stability, or the conduct of information operations (to include mis/disinformation campaigns, covert and overt support to political parties, COVID-19 related actions, and so on).

That's where automation comes in! Something I *am* good at is the establishment of a comprehensive analytic framework for understanding the use of cyber warfare as a policy implementation tool. Specifically, I built this framework into three phases, or 'Modes' as follows:

- **Mode 1** is a historical deep dive, tracing how a nation changed over time. It breaks history into periods based on leadership shifts, external events, tech milestones, and societal tensions. The overarching goal is to identify common themes or narratives that emerge and have continuing implications in modernity, particularly as related to leaders' decision-making. Analysis includes:
    - *Internal Dynamics*: How changes in power, society, and the economy shaped public views of tech and the government's focus on surveillance vs. digital openness.
    - *External Relationships*: Did alliances lead to tech transfer or did isolation drive homegrown solutions? Was cyberwarfare a factor in foreign relations?
    - *Values & Control*: How evolving views on freedom, privacy, etc., may have driven increased state surveillance or online restrictions.
    - *Tech Infrastructure*: Focus on how the state influenced the development of open tech VS tightly controlled systems, revealing its evolving priorities.
    - In later years, *Cyber Events*: Public reactions to hacks, policy shifts, etc., show if they increased support for state cyber defense or greater restrictions.

- **Mode 2** creates leader profiles to uncover how their beliefs and backgrounds affect their willingness or interest in various policy creation and implementation, to include how they drive cyber warfare strategy. The focus is on policy influencers across government, defense, and tech sectors. Analysis examines education, past roles, ideology (via public stance on cyber), and power networks to see who has sway. External influence on leaders is mapped via foreign ties, tech reliance, and links to cyber experts abroad. Where possible, it includes factors like digital literacy, responses to attacks, and policy think tank connections. Mode 2 emphasizes careful vetting of open-source information to avoid bias in these profiles.

- **Mode 3** is the 'meat and potatoes' of analysis, here, pulling away from simple information collection and really layering the data from Modes 1 and 2 to understand the total circumstance in which a leader is making decisions. Consider a trip to the grocery store – it's not just 'I need bread'; it's 'I

need bread; I'm running late for school pickup; what's my checking account balance; do I have jelly; etc.' and similarly, a given decision is not occurring in a vacuum. Leaders are implementing policy with pressure from other government, defense, industry actors, from the constituents, from external actors and world events, and so on. We can only account for so much of this, but what we *can* account for is how, psychologically, a leader reacts to stress. In the US Marine Corps, a similar analysis is DRAW-D- used to understand the enemy's most likely course of action.

More concretely, Mode 3 analyzes a nation's likely cyber espionage targets by uncovering motivations in leadership rhetoric. The focus is on how leaders link tech gaps, perceived threats, and adversarial relationships to espionage goals. Analysis scrutinizes leadership statements for:

- *Blame*: Do they link sanctions or other foreign pressure to stalled innovation? This hints at R&D focus OR a willingness to seek knowledge via espionage.
- *Urgency*: Does the discussion of rivals' tech progress suggest a need to copy those advances, whether through legal or covert means?
- *Retaliation*: Accusations of IP theft by potential targets signal areas of vulnerability, or industries they may try to target in response.

Fortunately, LLMs are good at each of these modes when given substantial parameters and guidelines. In creating this guide, I used both Google's Gemini (formerly Bard) Ultra 1.0 and OpenAI's ChatGPT4 – to include standing up my own GPT modes. I was concerned about bogging down the systems in processing a huge amount of data, nor did I want to introduce space for inclusion of respective nations' information operations, so the level of detail is not as deep as theoretically possible; the analysis is substantial.

I had several iterations of this due to a catastrophic loss of data in Gemini (when it told me, unprompted, how to circumvent Google's link filtering), but basically for both Mode 1 and Mode 2, I took the output from one tool and passed it through the other tool for validation, sometimes more than once, to use a 'law of averages' approach to ensuring reasonable accuracy, while also **almost completely removing human analyst bias** in final outputs – I never manipulated the data myself, instead instructing the tools to filter and prioritize their own data.

For Mode 3, I started with a custom GPT and attached a .pdf document that contained the final Mode 1 and Mode 2 information as GPT's primary dataset. I asked for insights and predictions, 'anti-predictions' that were unlikely to occur, and important trends to consider that could break either direction with significant second or third order effects.

Overall, I'm satisfied with the quality and depth of this product, and I think this sets the base for future expansion of these LLMs as analytic tools beyond how I've seen them used before.

I chose to use GUI interactions rather than manual API calls mostly because I didn't want to focus on the tech; I wanted to focus on automating meaningful analysis. I will explore this change in the future.

What follows is a quick reference to cyber-related geopolitical decision-making for the upper echelons of the government of Iran, to include Ali Khamenei and Ebrahim Raisi. I have about ten more pages of data from all Modes (it got abstracted away in the summarization process) – happy to share with the curious.

I'm happy to address information gaps and analytic shortcomings of this product in detail. Reach out. Of note, I begged for probabilistic language but could not get the tools to implement, regardless of what I said to them – including providing a chart, descriptions, and examples.

Important Analyses

Affirmative Insights

These are likely motivators for Iranian leaders' decision-making and risk calculus.

- **Sanctions as Catalyst:** Sanctions drive Iran's focus on breaking technology barriers through cyber espionage and independent development.
- **Focus on Adversaries:** Western rivals spur Iran's sense of urgency, making it prioritize matching or exceeding their cyber capabilities.
- **IP Concerns:** IP theft accusations pinpoint areas Iran considers vital for both defense and gathering actionable intelligence to close capability gaps.

Unlikely Outcomes

These are issues unlikely to occur based on analysis rooted in historical narratives and considered through a lens of modern contexts.

- **Unprovoked Attacks:** Iran is unlikely to strike neutral/allied states; focus remains on perceived Western adversaries.
- **Public Attribution:** Iran will maintain deniability in cyber operations for diplomatic advantage and tactical flexibility.
- **Contradicting Values:** Actions undermining core Islamic principles are improbable – even offensive ops are framed to fit their narrative.
- **Wholesale Western Adoption:** Indigenous tech development and the "halal internet" signal limited direct use of Western tech is improbable.
- **Abandoning Cyber Sovereignty:** Censorship, surveillance, and local tech development are too central to control, unlikely to decline.
- **Shifting to Conventional Only:** Iran sees cyber capabilities as vital; a large-scale reduction or trade-off is highly unlikely.

Issues to Watch

These issues are critical to how Iran handles policy implementation - both domestic and foreign - and could break either way. It will be important to monitor related topics and re-evaluate these later.

- **Shifts in Strategic Alliances:** Iran's alliances with Russia and China are crucial, providing tech and diplomatic support to bypass Western sanctions and bolster its cyber capabilities. Changes in global geopolitics – new conflicts, agreements, or shifts in these nations' policies towards Iran – could significantly alter the level of support received, directly impacting Iran's cyber strategies.
- **Impact of International Sanctions on Cyber Capabilities:** Sanctions have made Iran prioritize cyber capabilities as asymmetric warfare to counter conventional disadvantages. Targeted by cyber espionage and attacks (like Stuxnet), Iran has crafted a sophisticated cyberwar organization built on its experience in covert ops. It leverages units like the IRGC and the Basij for a potent proxy hacker force, demonstrating significant growth despite restrictions.
- **Internal Political Dynamics and Cyber Policy:** Iran's cyber policy reflects the power of hardliner factions (like the IRGC) who use offensive operations against adversaries and internal surveillance for control. Sanctions and the elite's focus on regime preservation likely motivate the use of cyber capabilities for both external coercion and tightening internal control. Emphasis on indigenous tech aligns with hardliner desires for sovereignty and resisting Western influence.
- **Global Norms and Regulations on Cyber Activities:** Currently, a lack of clear international cyber norms allows Iran flexibility in operations. Evolving UN discussions could establish rules limiting state actions and isolating those who don't comply. Iran may need to strategically adapt its cyber tactics based on the outcome of these norms or risk greater international scrutiny.

Contexts and Considerations - What Matters?

Cyber Sovereignty & Cultural Control in Iran

Iran's leadership champions cyber sovereignty as a means of suppressing dissent and preserving its ideological narrative. Khamenei's emphasis on a "halal internet" prioritizes control over Western influence, leading to censorship and blackouts during periods of unrest. This domestic focus contrasts with Iran's more aggressive external cyber actions targeting adversaries. Sanctions drive indigenous tech development for tighter control, while growing reliance on encrypted communication challenges surveillance, prompting a need for new tactics or tools.

Control & Its Erosion: Navigating the Digital Age

Iran's leadership views the internet as a threat to its control over information and public narrative. The erosion of traditional control mechanisms by online platforms fuels the regime's fear of dissent and the spread of Western influence undermining core values. This tension shapes strategies aiming to restrict internet access and promote a national intranet, highlighting the battle between digital connectivity and the regime's desire for absolute control. Iran's approach reflects a broader struggle faced by authoritarian regimes – balancing the need for technological progress against anxieties about preserving internal power and societal traditions.

External Forces: Navigating Pressure and Opportunity

Iran's leadership strategically frames external threats to unify the public against perceived Western adversaries. This tactic leverages historical grievances and sanctions to redirect blame for domestic hardship outward, solidifying control. External engagement is a necessity for technological progress, but the regime fears open connectivity which challenges its narrative and creates opportunities for dissent. Sanctions fuel mistrust of foreign technology and justify increased censorship and surveillance under the guise of national security. Iran's external challenges thus have profound internal consequences, driving its restrictive digital policies and framing national identity against foreign pressure.

Technology: Balancing Modernity and Traditionalism

Iran's leadership seeks to balance technological advancement with the preservation of traditional Islamic values. While recognizing the need for digital literacy and economic advantages, the regime fears unrestricted internet access as a threat to its ideological control. The concept of a "halal internet" aims to secure the benefits of connectivity while heavily filtering content, ensuring technology doesn't erode the regime's power. This vigilance extends even to platforms from other Muslim nations, revealing internal power struggles over interpretations of acceptable content. Iran's approach to technology reflects a desire to leverage these tools to reinforce control, while managing anxieties about societal change and challenges to its narrative authority.

Generational Dynamics and Digital Divides

Iran's youth, digitally connected and globally aware, challenge the regime's desire for tight narrative control. The internet provides space for self-expression and alternative viewpoints outside of state-sanctioned channels. This generational divide forces the regime to balance suppression (which risks alienating young Iranians) against allowing greater online freedom (which could erode the regime's power). The leadership adapts tactics for online control to reflect this tension, emphasizing its awareness of the potential for technology to facilitate discontent and societal change.

Evaluating Leader Motivation & Risk Calculus

Important Internal Dynamics

- *Hardline Dominance*: Khamenei and Raisi enforce strict control over the digital sphere for ideological conformity and to quell dissent. They champion surveillance, censorship, and a restrictive "halal internet".
- *Reformist Resistance*: While limited, voices urging for greater openness exist within the government. They recognize the economic potential of digital technology and may subtly influence aspects of policy implementation.
- *Military Role*: The IRGC's involvement in both external cyber operations and internal surveillance blurs the line between national security and control. This could lead to adaptation of offensive tools for harsher domestic surveillance.

Leader Profiles

Ali Khamenei, Supreme Leader of Iran

Background: Shaped by Islamic jurisprudence and philosophy, Khamenei's leadership coincided with the expansion of Iran's cyber capabilities. This reflects their strategic importance for defense and power projection.

Ideology: Advocates strong cyber defense to counter Western influence and threats. Promotes a "halal internet" to protect Islamic values and limit dissent. Views cyber capabilities as both defensive and offensive tools.

Power & Influence: Khamenei wields supreme authority over cyber policy. Self-reliance drives development and deployment of cyber tools. Internal surveillance often linked to perceived instability. Foreign cyber relations are complex – driven by alliances against shared enemies, but also influenced by active retaliation against competing interests.

Ebrahim Raisi, President of Iran

Background: Raisi's rise from the judiciary reflects his hardline stance on Islamic law and suppression of opposition. This background suggests a commitment to maintaining social control, likely extending to the cyber domain.

Ideology: While less outspoken on cyber policy, Raisi likely aligns with Khamenei. *Expect*:

- Increased surveillance and censorship under the guise of security and morality.
- Focus on domestic tech development to build more restrictive tools and avoid sanctions.
- Deployment of offensive cyber capabilities for regime preservation, even at the expense of foreign relations.

Power & Influence: Raisi is responsible for implementing Khamenei's cyber directives. His influence is likely seen in:

- Enforcing a strict vision of the "halal internet", likely through harsh punishments.
- Strengthening cybersecurity partnerships with nations like Russia and China who share similar views on digital control.

Other Internal Stakeholders

- *Islamic Revolutionary Guard Corps (IRGC)*: Blurs lines between external cyber capabilities and internal surveillance, granting unusual power to influence both policy and citizen control. Salami's rhetoric on cyber threats needs scrutiny to identify inflated justifications for domestic oppression.
- *Supreme Council of Cyberspace*: Dictates cyber policy for Khamenei. Prioritizes control, shaping technical limitations and societal impacts. Contests with the ICT Ministry reveal fluctuations in Khamenei's internal control vs economic growth goals.
- *Ministry of Intelligence*: Focus on surveillance extends from foreign espionage to domestic dissident suppression. Critical to distinguish legitimate security threats from regime's targeting of internal critics.

External Relationships

Strategic Alliances

- **Russia:** Joint cyber initiatives on defense and intelligence sharing. Russia provides technology and expertise to bolster Iran's capabilities.
- **China:** Comprehensive partnership includes technology exchange supporting cyber advancement. Iran's role in the Belt and Road Initiative fosters digital infrastructure development.

Adversarial Relations

- **United States:** Iran implicated in cyberattacks against U.S. interests. Stuxnet attack fueled Iran's development of offensive and defensive cyber capabilities.
- **Israel:** Ongoing cyber conflict focused on espionage and attacks on critical infrastructure.
- **Gulf States:** Iran conducts disruptive cyberattacks (ex: Shamoon virus against Saudi Aramco) within the broader context of regional tensions.

Historical Trends as Explanatory Information

Pre-Modern Period

Domestic Dynamics: During this era, Iran was ruled by successive dynasties, most notably the Safavid (1501-1722), Afsharid (1736-1796), Zand (1751-1794), and Qajar (1789-1925) dynasties. These periods were characterized by centralized monarchical rule, with a strong emphasis on Persian culture and Shia Islam as defining elements of the state. The domestic dynamics of these times were marked by court intrigues, tribal politics, and periodic conflicts with rival powers.

External Relationships: Iran's strategic location made it a focal point of contestation among emerging European empires, the Ottoman Empire, and neighboring Russian and Central Asian powers. These external pressures often influenced Iran's internal politics and its approach to governance, military strategy, and economic policies.

Societal Values & Tensions: Society in pre-modern Iran was structured around a feudal system, with a significant rural population living under the control of local landlords and a tribal system. Urban centers

were places of trade, craftsmanship, and cultural production, but also of political and religious authority. The period was marked by a deep entrenchment of traditional values, with the clergy playing a crucial role in society.

Technological Infrastructure: Technological advancements during this period were limited and focused mainly on agriculture, military, and some aspects of communication and construction. There was little in the way of infrastructure that would later directly influence cyber policies, but the foundations of governance, control, and the central role of the state were firmly established.

Constitutional Revolution to Pre-Revolution Modernization

Domestic Dynamics: The Constitutional Revolution (1905-1911) marked a significant turning point, establishing a parliament and formally limiting the monarch's powers. This period saw the struggle between modernist forces seeking to reform Iran along Western lines and traditional elements wishing to preserve the Islamic and monarchical order. The Pahlavi dynasty (1925-1979) pushed for rapid modernization and secularization, significantly altering Iran's social and economic landscape.

External Relationships: Throughout the 20th century, Iran's relationships with foreign powers, notably Britain, Russia, and later the United States, had a profound impact on its internal development. The discovery of oil in the early 20th century transformed Iran into a strategic geopolitical player, leading to increased foreign involvement in its domestic affairs, especially in the 1953 CIA-MI6 coup that reinstated Shah Mohammad Reza Pahlavi.

Societal Values & Tensions: The push for modernization under the Pahlavis created societal tensions, as rapid urbanization, education, and the promotion of Western values clashed with traditional Iranian culture and religion. These tensions were exacerbated by the Shah's authoritarian governance and the suppression of political dissent, setting the stage for the Islamic Revolution.

Technological Infrastructure: The Pahlavi era saw significant investment in infrastructure, including roads, telecommunications, and industry, laying the groundwork for future technological advancements. While not directly related to cyber policy, these developments contributed to the creation of a more connected and technologically aware society.

Pre-Revolutionary Period

Domestic Dynamics: Before the 1979 Islamic Revolution, Iran under Shah Mohammad Reza Pahlavi was moving towards modernization and Westernization, with significant investments in education, industry, and technology. However, the Shah's authoritarian regime, reliance on the secret police (SAVAK), and close ties with the West, especially the United States, led to widespread dissatisfaction.

External Relationships: Iran's strategic alliances with Western powers, particularly the US, facilitated access to advanced technology and military equipment, including early computing technology. However, these relationships also became a source of internal tension and a rallying point for opposition groups.

Societal Values & Tensions: The rapid modernization efforts and the overt Western influence led to societal tensions, with traditionalist and religious groups feeling alienated. This period saw a clash of values between modernity and tradition, setting the stage for the Islamic Revolution.

Technological Infrastructure: Technological advancements were primarily driven by state initiatives focused on modernization and economic development. While there was investment in technology, it was not yet a central focus of governance or societal interaction.

Post-Revolution Period

Domestic Dynamics: The 1979 Islamic Revolution dramatically shifted Iran's political landscape, establishing an Islamic Republic. The new regime prioritized Islamic values, leading to significant changes in governance, social policies, and a reevaluation of Western influence, including in technology.

External Relationships: Post-revolution, Iran found itself increasingly isolated internationally, especially after the US Embassy hostage crisis. The Iran-Iraq War (1980-1988) further strained resources and highlighted the importance of self-reliance in defense, including in emerging areas like cyber capabilities.

Societal Values & Tensions: This period was marked by the consolidation of the Islamic Republic's power, with strict control over societal values and media. There was less emphasis on the aggressive pursuit of technological modernization in favor of cultural and religious consolidation.

Technological Infrastructure: Despite international isolation, Iran continued to develop its technological infrastructure, albeit more slowly and with a focus on independence from Western technology sources. The Iran-Iraq War underscored the importance of communications and intelligence in modern conflict, laying the groundwork for future interest in cyber capabilities.

Early Internet Age

Domestic Dynamics: Iran's approach to the internet was initially cautious but grew more interested as the potential for economic development and information dissemination became apparent. The government began to invest in internet infrastructure while also putting in place mechanisms to control and monitor online activities.

External Relationships: Despite continued international tensions, Iran engaged in limited technological exchanges through non-Western partners and focused on developing indigenous capabilities, including in the field of cyber technology.

Societal Values & Tensions: The internet opened new fronts for societal debate and conflict, with the government implementing censorship and surveillance to maintain control over the narrative and suppress dissent.

Technological Infrastructure: The expansion of internet access and mobile technology began to transform Iranian society, with the government balancing between leveraging these tools for economic and educational purposes and controlling them to prevent unrest.

Rise of Cyber Capabilities

Domestic Dynamics: Recognizing the strategic importance of cyberspace, Iran has significantly invested in its cyber capabilities, both for defensive purposes and to assert its influence regionally and globally. The Green Movement in 2009 highlighted the internet's role in mobilization and dissent, leading to increased government focus on cyber surveillance and control.

External Relationships: Iran's cyber capabilities have also been shaped by its confrontations with Western countries, especially the United States and Israel, including notable cyber incidents such as Stuxnet. These confrontations have driven Iran to further invest in cyber warfare and defense capabilities.

Societal Values & Tensions: The government's tight control over the internet and social media, including blocking and filtering content, has led to tensions within society, with many citizens seeking ways to bypass censorship. This dynamic reflects a broader struggle between the desire for connectivity and freedom of expression versus the state's focus on security and control.

Technological Infrastructure: Iran has developed a sophisticated infrastructure for both exploiting the benefits of the digital age and maintaining strict oversight. This includes significant advancements in domestic internet infrastructure, such as the National Information Network, aimed at enhancing control over online content while also seeking to safeguard against external cyber threats.