CERIAS

The Center for Education and Research in Information Assurance and Security

Cyber Conflict Capabilities Assessment: Islamic Republic of Iran

Jake Kambic, Dr. Samuel Liles

Abstract

The purpose of this study was to perform a topical OSINT analysis of Iran's capability to engage in cyber conflict. The capabilities were assessed on an ordinal Likert-type scale which seeks to independently grade a nation-state's cyber capabilities in a general way. The metrics used were intended to gauge both the offensive and defensive resources available to a country within the cyber domain. These metrics are as follows:

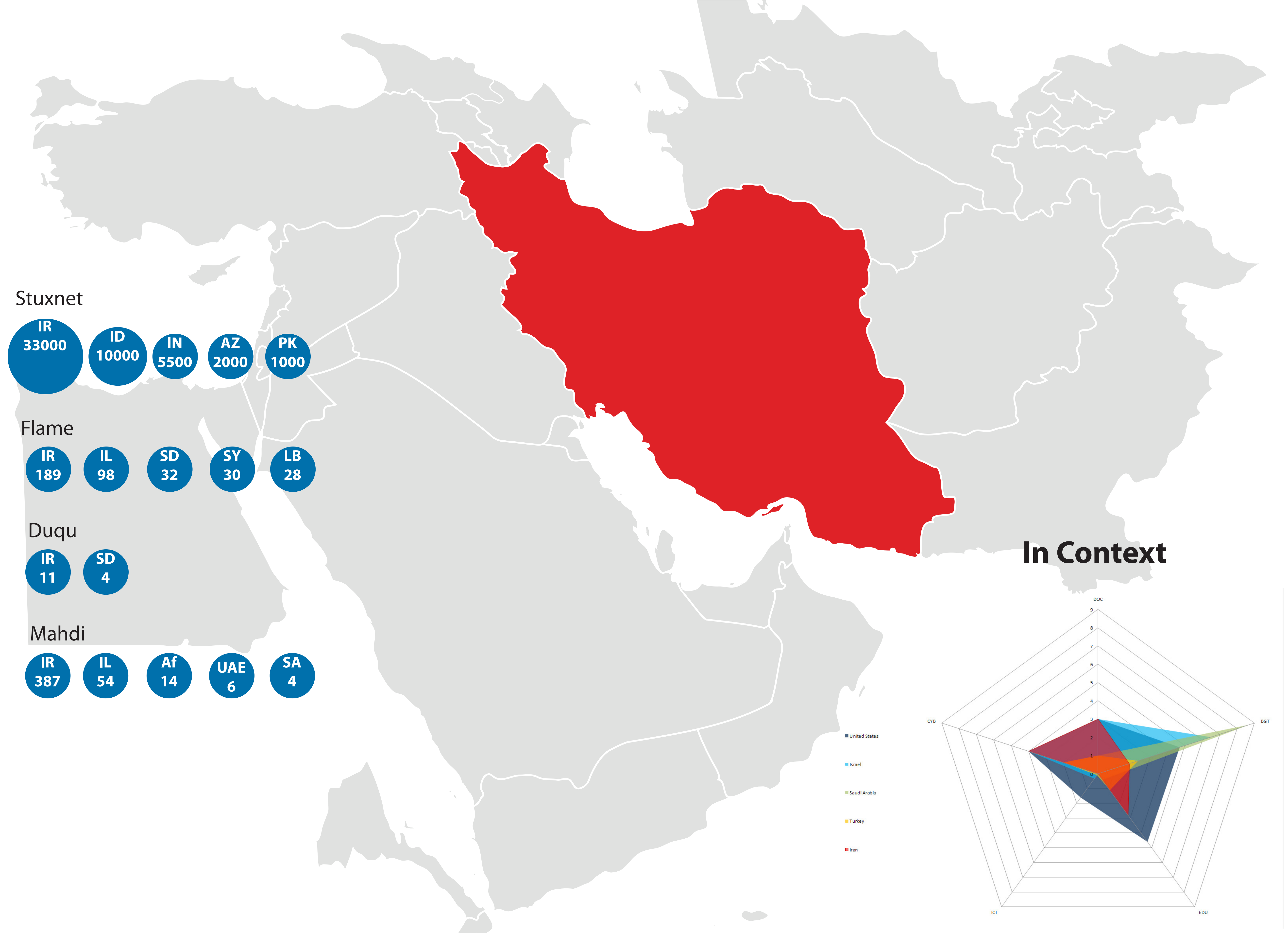
1. **References in Doctrine or Organization Structure** (Asymmetric doctrine, cyber warfare specific doctrine, dedicated cyber warfare units or affiliates) [DOC]
2. **Areas of Gov't/Military Spending** (In particular Education, Technology Research, ICT, EMS weapons, conventional weapons, and defense spending as a percentage of GDP) [BGT]
3. **Development of Operational Assets** (Number of university programs studying relevant fields, number of collegiate students, number of ICT companies/specialists) [EDU]
4. **Number of ICT assets/assets per capita** (Overall attack surface and cultural acceptance of technology) [ICT]
5. **Number/Severity of Cyber Security Incidents** (both offensive and defensive) [CYB]

Because the information was gathered via OSINT, sources observed and used may introduce their own biases and at times the provenance of the information could not be independently verified.

Likely Incapable	Likely Immature	Likely Capable	Demonstratively Capable	Demonstratively Proficient
Has not demonstrated the resources or organization	Has some development of the identified resources and formation of organization	Has the resources, willingness, and organization to be successful in at least a limited capacity	Has demonstrated the resources, willingness, and has engaged in cyber conflict activities with at least limited success	Has demonstrated the advanced resources, willingness, and successful engagement of cyber capabilities to a high magnitude of effect and accuracy

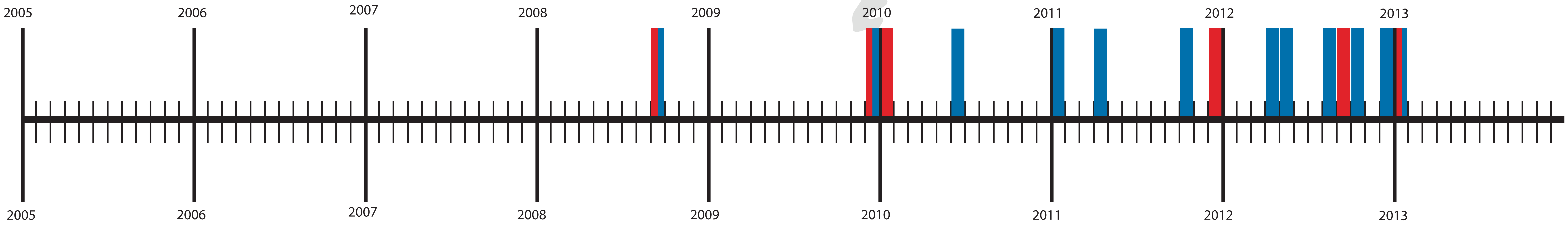
Cyber Conflict Defined

The conduct of large scale, politically motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks, and infrastructures, including the use of cyber-based weapons or tools by non-state/transnational actors in conjunction with other forces for political ends. [1]



Iranian Cyber Events

Offensive 🟥
Defensive 🟦



References
[1] Mulvenon, J. & Rattray, G. (2012) Addressing cyber instability. Cyber Conflict Studies Association. Retrieved from http://www.cyberconflict.org/storage/CCSA%20-%20Addressing%20Cyber%20Instability.pdf