Cyber Security Differences Between States and Resistance Movements

Patrick D. Allen, COL (Ret'd) USAR, Associate Editor Cyber Defense Review from West Point Press. This article was published on The Resistance Hub 20 March 2026, and updated on 12 April 2026.

Abstract

Every organization today needs cyber security, as well as methods to test and ensure that security is achieved. For State security organizations, the ability to manage cyber security assets, monitor data, check and test compliance, and train staff can be centrally and efficiently managed. However, when Resistance Movements need to use a cellular organizational structure for physical and informational security, these cyber security functions need to be distributed. Resistance Movements also need to avoid compromising multiple cells due to using shared cyber assets. This article presents the differences between cyber security for both the State and a Resistance Movement, and techniques Resistance Movements might take to compensate for the need to distribute these security functions.

Background

Some of the material in this short article is excerpted from examples described in Chapter 4 of the publication *Resistance and the Cyber Domain*, from the US Army Special Operations Command series Assessing Revolutionary and Insurgent Strategies (ARIS), which this author co-authored in 2019.[1] This article includes updates since the time of that publication.

Cyber Security Compliance

Organizations need to ensure that security policies are being implemented correctly. For example, if a security patch or update is required for cyber equipment (including smart phones), then independent confirmation checks need to be made on the devices rather than simply relying on the users to install the updates. In a similar manner, using an appropriate encryption mechanism for communications is essential to cyber security. Passwords and PINs need to be confirmed to have a certain length, not be predictable, and have a specified lifespan. Alternatively, if policy allows, one can use multi-factor authentication (MFA) instead of relying on password change frequency for security. "Testing and enforcement of the security of the cyber capabilities used by a resistance movement or a state security service are just as important as physical testing and enforcement of member loyalty."[2]

For State Security organizations, Unified Endpoint Management (UEM) and similar systems can be operated from a central location to monitor compliance of all devices assigned to it. The ability for the UEM to reach out to all assigned devices to determine their compliance status is a great benefit to State Security organizations. MFA can be set up for each application or website. Centralized software is also available to State Security to monitor password strength and duration if so desired.

In contrast, Resistance Movements that rely on cellular organizational structures do not have the opportunity to use a UEM system. If they were to use a UEM, then if it were compromised, the whole organization is compromised. The same situation applies to password strength checking. In general, centrally managed security software is not an option for Resistance Movements.

Resistance Movements can use MFA since it is application-specific, but care needs to be taken to ensure that the application itself has not been compromised. If compromised, then anyone logging into that application even with MFA could be compromised.

Resistance Movements also need to avoid compromising multiple cells by using single shared cyber assets. For example, the Syrian Resistance Movement fighting against the Assad regime used shared computers for satellite-based Internet access due to resource constraints. This caused many assets across multiple cells to be compromised by the State Security forces and their allies.[3]

Although less efficient and definitive, the leader of each Resistance cell could simply send its members reminders to perform the upgrades or password changes. While not as efficient or dependable as a centralized, automated system, it may be adequate for a Resistance Movement's purposes.

Real Time Cyber Security Monitoring and Response

Due to the benefit of having centralized data collection across the network, State Security can leverage Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems to be able to quickly respond to detected threats on their assets, and to ensure that its users do not go to dangerous sites. Moreover, they can quickly and frequently update the list of dangerous sites when new ones are detected. In addition, they can identify locations in the network where suspicious activity is occurring, and can also respond to detected anomalies by isolating parts of the network while being investigated further.

Resistance Movements do not tend to have centralized data collection from their network, as that would constitute a single point of failure for the whole organization. Keeping the cellular structure intact precludes the ability to benefit from centralized monitoring and threat response. At the same time, the cells are already "isolated" on their part of the cellular structure, so isolating the threat is less important unless the threat can jump from cell to cell. The use of air-gap jumping malware still remains a problem for Resistance Movement cells,[4] as well as any shared resources as described above.[5]

At the cell level, neither the cell leader nor its members have the cyber skills or software necessary to identify new or evolving threats on their assets. Moreover, a Resistance Movement has no efficient or timely means of adding newly discovered dangerous sites to a block list.

Cyber Security Training

Cyber security relies heavily on users being trained in proper cyber hygiene, such as not picking up and using stray thumb drives,[6] not opening email attachments, not clicking on links in emails, or not falling for cat phishing attempts. (Cat phishing is usually where a supposedly beautiful woman shows interest in a user in order to get them to unintentionally load malware onto their system.)

State Security organizations can centrally plan, test and monitor cyber security training events. In addition to computer-based training, the organization can send out "test" phishing emails to see who clicks on them and then require additional training for those who need it.

Sending test cat phishing attempts can also be useful. State Security forces have been successfully exploited by cat phishing. In 2017, hackers supporting Hamas sent cat phishing

messages to Israeli Defense Force personnel and successfully compromised a number of systems.[7,8] In a similar manner, unknown hackers have used "attractive Ukrainian female profiles" as cat phishing to encourage Russian soldiers to commit acts of sabotage before defecting.[9] Both phishing and cat phishing have continued to be successful attack vectors that requires organizations to be vigilant and constantly train against this threat.

Resistance Movement members must also be trained in these proper hygiene techniques. For example, the Syrian Resistance Movement members were sent cat phishing emails that, after the user followed instructions from the hacker, ended up receiving malware embedded in pictures that compromised their devices.[10] This can be particularly problematic if the Resistance Movement uses shared cyber resources, as described above.[11]

To help compensate for the lack of centralized training and testing capabilities, a Resistance Movement could create and distribute a "kit" to each cell leader to allow the leader to send computer-based training to its members, as well as test phishing and cat phishing messages. The cell leader would be responsible for the training and testing of the members of their cell. While not efficient, this at least could provide some cyber security training, testing and oversight.

Cyber History Background Checks for Recruits

Both State Security and Resistance Movements need to "vet" their recruits by doing background checks. This is a standard security procedure to make sure the recruit is genuine and not an enemy plant.

State Security can centralize their background checks and use a wide range of sources to determine the trustworthiness of their recruit. There are many commercial companies that provide national and international background checks for a fee. The amount of open-source information available about anyone is continuing to increase over time. One area of particular interest to State Security is whether the recruit has visited the websites supportive of Resistance Movements. State surveillance capabilities can encompass a wide range of communication channels, including phone, social media, and other Internet connections. Authoritarian states do not need proof to arrest and interrogate someone on suspicion of being a resistance member.

The Resistance Movement has all of the above concerns, but the vetting process is not centralized. Even more of a concern to the Resistance Movement is the fact that phony websites purporting to support the Resistance Movement may have been set up by State Security.[12] As a result, a genuine recruit may have already been compromised by visiting a phony website set up by State Security. This means that the recruit has already been identified by State Security as a potential member of the Resistance Movement. Therefore, part of the vetting process by the Resistance Movement cell is to find out which websites the recruit previously visited. If the recruit visited one or more of these phony websites, they are already compromised and should not be recruited.

Summary

Resistance Movements need to be cognizant of the limitations facing them in the area of cyber security. Both State Security elements and Resistance Movement cells need adequate cyber security in order to survive. However, State Security elements have a significant advantage over

Resistance Movement cells because their cyber security capabilities can be efficiently centralized.

Moreover, cyber security expertise is fairly rare in any organization. In State Security organizations, these tend to be in a central location. Conversely, Resistance Movements cannot afford to place all of their cyber security personnel in the same location or organization. Moreover, neither cell leaders nor their members tend to be cyber-savvy. As a result, they may not be able to achieve the basic security practices described in this article. Cases of successful cat phishing are an example of this.

While there are a few work-arounds for a Resistance Movement, the cellular structure of the organization requires the burden of ensuring cyber security to be on the cell leader. If equipped with a software toolkit, the cell leader can provide computer-based training to cell members, as well as send out test phishing and cat phishing emails and texts. While less efficient than centrally managed capabilities, this does provide some cyber security benefits.

Resistance Movement cyber security is also less efficient due to the lack of being able to monitor cyber traffic for anomalies across distributed networks. This makes it difficult for a Resistance Movement to detect when some of their assets are compromised. While the cellular structure can keep the cyber compromise localized, if a Resistance Movement uses shared cyber resources, the cellular structure no longer provides protection via isolation. Shared resources means that members of a cell may be sharing state-distributed malware and be surveilled on their shared assets.

Overall, Resistance Movements inherently face greater risks in cyberspace than State organizations. One option for them to consider is to perform resistance activities using old-school analog techniques, such as paper materials and face-to-face meetings. Analog techniques carry their own risks, but there is a long history of how to use them successfully. While members of the Resistance Movement do not want to completely eliminate their personal digital presence entirely (for that might also be suspicious), limiting all or most resistance-related activities to analog techniques could reduce the digital risks in modern cyberspace, especially within an authoritarian state.

---

[1] Ryan, Kristen, ed. 2019. Resistance and the Cyber Domain. U.S. Army Special Operations Command series Assessing Revolutionary and Insurgent Strategies (ARIS). August, 2019. https://theresistancehub.com/wp-content/uploads/2025/09/ARIS_Resistance_CyberDomain.pdf.pdf

[2] Ibid., p. 97.

[3] Regalado, Daniel, Nart Villeneuve, and John Scott Railton. 2015. Behind the Syrian Conflict's Digital Front Lines. *FireEye Threat Intelligence Special Report*, February 2015, p. 14. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf

[4] For example, infected thumb-drives can contain malware that could infect cyber assets not connected to the Internet. William J. Lynn. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, Sept/Oct 2010. https://apps.dtic.mil/sti/citations/ADA527707.

[5] Regalado, Ibid.,

[6] Lynn, Ibid.

[7] Goldman, Paul and Alistair Jamieson. 2017. Hamas Used Fake Social Media Accounts to Hack Israeli Soldiers' Phones: IDF. *NBC News*,12 January 2017. https://www.idf.il/en/mini-sites/hamas/hamas-uses-fake-facebook-profiles-to-target-israeli-soldiers/.

[8] Petronella Technology Group. Israeli Soldiers Hacked by Fake Social Media Profiles. https://petronellatech.com/israeli-soldiers-hacked-by-fake-social-media-profiles/.
[9] Combellick, Dylan,. 2014. Ukraine Update August 6. Medium.com, 6 August 2024. https://medium.com/@dylan_combellick/ukraine-update-august-6-8c72a3cd7d8a.
[10] Regalado, Ibid., p. 12.
[11] Regalado, Ibid., p. 14.
[12] Regalado, Ibid. p. 13.