

Editorial note - This blog post is part of our Scribbles series. If interested in submitting creative content, view our guidelines [here](#) or contact Cassie Crosby at cassie@fromthegreennotebook.com.



By Aaron Utsler

Oliver sat in the drab wooden chair in the rear of the Executive Conference Room. The Division Chiefs in their cheap, poorly tailored suits arranged along the oval extended table with the Director at the head. A complement of video monitors adorned the main wall with smaller satellite TVs along the sides of the room so the staffers could follow along. The carefully scripted presentation illuminated the monitors, having been carefully filtered by the various functional chiefs so as to shield the the Director from any intelligence notices that might challenge the narrative espoused by the machine in Washington. Another useless update brief. Another opportunity for the bureaucratic hacks to deepen their rice bowls, he thought to himself.

Oliver now found himself reassigned to the Dungeon's headquarter's staff. A menial position disguised as career progression. The truth of it is that the assignment was punishment after a verbal altercation with the Patriarch turned physical while assigned to the House in Doha. The Dungeon was the pejorative term used by field operatives for the National Intelligence Agency's headquarters in Washington D.C. Houses were the outstations positioned around the globe to act as the eyes and ears of Washington.

A lot had changed since the fast paced counter-terror missions of the earlier years of the 21st century. It was 2065 but it might as well be 1965. A new Cold War guided geopolitical thought and behaviors in the world. The globe was once again divided into East and West with small enclaves in one hemisphere aligned with dominant hegemony in the other. Like its predecessor a century earlier, the U.S. and Russia dominated the lesser states. America was overstretched fighting religious zealots across two continents and Russia sought to regain the former glory of the czars as the regime fought to annex the Crimean and bolster its Syrian puppet.

During the proxy wars of Iraq and the Ukraine in the earlier part of the century, the U.S. and Russia played an aggressive game of brinkmanship which resulted in a number of miscalculations. Fearing the fall of a strategic partner in Syria by the hands of U.S. backed irregulars, Russia, working through Iranian clients, sponsored an offensive cyberattack on the American banking system. The fallout led to a run on the banks resulting in the near collapse of the economy and a depression lasting decades. In the fervor of the counterattack, the U.S. lashed out on the Russian critical infrastructure. The parry was meant to deprive the czarists of basic services; however, the lack of fail-safes in the Russian government meant a full scale meltdown of the power grid to include decrepit nuclear facilities. If the West's collapse looked like a resurrected Great Depression, then the East entered a new Dark Age. The decrement of both nations affected the global distribution of power, bringing strength in many cases to the once developing world. China and Japan

emerged as technological powerhouses aligned with Russia and America, respectively.

Both nations had retreated behind national borders for a time. The consequences of a poorly planned cyberattack led to a complete reallocation of funding and resources. Without adequate funding, the American military shrank to all time lows. Washington streamlined the intelligence functions of once disparate entities into the consolidated National Intelligence Service which included both a foreign and domestic section with the military as the action arm of the service. Similarly, Russia rebuilt the old KGB, this time with capabilities to defend and attack in the cyber world. National legislation passed, limiting the introduction of technology from one side into the other. A Digital Curtain separated the two political hemispheres.

In the interceding years, the Superpowers regained their position as leaders of the world. Because of the refocusing on technological prowess, the Digital Arms Race rapidly rebuilt economies the world over. The newly formed cyber industrial complex boomed creating jobs, grew revenue, and exponentially accelerated the fields of biometric monitoring and offensive-defensive software programming. The legislation forbidding the cross pollination of programs meant that neither side could adequately monitor the other. Defensive programs advanced to the point where even a skilled hacker could not penetrate the net for more than a few minutes with only minimal disruption to the home system. Russian Internal Security elements cracked down on local threats with all the viciousness of Stalin's Red Army. Gulags reemerged as the punishment du jour if executions were lenient on the offender.

Code decryption and monitoring became the staples of the intelligence world. Working through the less advanced client states of the adversary to infiltrate the mother network without the need to enter the denied areas of Russian sovereign boundaries were the bread and butter of the Houses. These networks were deemed less secure and less likely to be equipped with the same level of protection as Moscow's server would rate. These

assessments were made by the analysts back at the Dungeon, predicated on the belief Moscow's true capabilities would be too classified to share with even the loyalist of puppet states.

The ultimate goal in Washington was to infiltrate Moscow's supervisory control and data acquisition systems (SCADA) and implant a sleeper code. This code would lay dormant attached to what is known as a Zero Day Flaw in the system. A Zero Day Flaw is a unique weakness or vulnerability in the software that is impossible to defend because it has never been patched. The problem with this approach is its limited utility since it is a one-time use weapon. Once an attack exposes the flaw, system's engineers can repair the damage and prevent further attack. For the management at the Dungeon, this means the strategic deployment and employment of a code along national systems whereby the Russians could not retaliate.

Uploading this code would require a person with access to the system with the natural ability to go behind the firewall to serve as a trigger for an attack since Washington would not be able to activate the attack remotely, undetected by Russia's cyber defense systems. Without proper planning, once triggered, the KGB could deftly narrow down the list of offenders. Brutal interrogations would ensue until the culprit was found. This type of tactic is what led to Oliver's reassignment to the Dungeon. The Patriarchs, that is the head of a particular House, routinely sacrificed the life of agents to probe the varying security measures. Lives of agents mean little to the paper pushers in management. Throughout his time in the field, Oliver saw more than one of his agents "burned" in the name of operational momentum. In reality, careerists and would-be politicians became more and more detached from the reality of their decisions. The faces behind the operational win had become nothing more than coded words on a cable. Those, like Oliver, were left to deal with the consequences of such actions. Though detached, Oliver knew such trade-offs could and would happen. But the cold, cavalier nature of management had begun to run counter to his own moral compass.

In the field, Oliver served as the COO or chief operating officer for the House. He managed a small portfolio of agents and oversaw the younger operators. At six-foot tall and one hundred and eighty pounds, headquarters work suited him poorly. He now managed the drudgery staff work and prepared talking points for the higher ups. Specifically, Oliver's team led efforts to hunt down and neutralize Hannibal Ibrahim, an Iranian freelance operator trained by the Russians. The Dungeon attributed the deaths of more than half of its Middle Eastern and African agents to him, as well as some of the more damaging attacks to banking nodes in U.S. allied western Europe.

Rumors of Ibrahim's presence along the Curtain's boundary in Tunisia began circulating in the deep web. These boundary states were a bit of a grey area for the larger intelligence services, always playing both sides against the middle in hopes of more money or support suppressing whatever local opposition group arose that day. Tunisia is as far west as Ibrahim had ever been known to travel. Half the analyst believed this indicated an impending attack of a catastrophic nature otherwise the risk wasn't worth the potential gain. The other half believed that Ibrahim intended to cross the Mediterranean into Europe for the purposes of defecting. Either way, no one could confirm he had actually entered Tunisia least of all the Tunisians. As a border state, Tunisia's digital infrastructure comprised a hodgepodge of Eastern and Western technology effectively allowing the Superpowers to monitor half the available data.

Having operated in Tunisia as a first year, management assigned Oliver to head the task force searching for Ibrahim. Once found, the task force was to capture him and bring him into Europe for questioning. Naturally, management expected Oliver to do this from the comfort of his small office. Acting as go-between with the House in Tunis and the Washington staff, Oliver fed what known biometric data he had on file for Ibrahim to the House in Tunis for passage to local authorities. The House spent a significant amount of money in Tunis to equip the city with fingerprint scanners at the ports of entry tied to the House's database. More money was spent outfitting the city's population center's with

cameras containing retinal scanning software. A personnel file smuggled out of Moscow was said to contain Ibrahim's retinal file for a comparison match. With any luck, it would be worth the money.

After two weeks, the House in Tunis sent back a match. Local police cameras caught Ibrahim driving toward a compound outside the city. According to local authorities, the compound belonged to a French born separatist named Antoine Malaki. Antoine leads a small but violent revolt against the government not known to favor either of the major powers. Oliver was unsure what Ibrahim would want with a nonpartisan revolutionary. Antoine used low tech tactics against the Tunisian government reminiscent of the wars in the earlier half of the century. Maliki's group was not believed to have any significant ties to the net nor did the group give much thought to the larger game played in Washington and Moscow.

Oliver advocated, successfully, for a raid on the compound. Using the local security force as a buffer, an elite strike force entered the compound. The team shuffled Ibrahim across the Mediterranean using stealth aviation. The Russians, having monitored the raid via their contacts, were equally curious as to why one of their top agents had traveled so far from the security blanket provided by their security service. The Russians were equally frustrated with losing visibility with their man once in Europe - deep behind enemy lines as far as they were concerned.

The interrogation team met the force on the Tarmac in London to take custody of the prisoner. During the course of the interrogation, Ibrahim revealed he had stolen a sensitive program from the Russian Research and Development Agency. The program acted as a sort of master key. It had the ability whether in an American or Russian based system to allow remote access to the network. Once in, it could ferret out every major Zero Day Flaw in the system and bring down multiple systems simultaneously. The really valuable component of the program is that it could enter the SCADA from any port. It didn't require the deep

penetration as in previous attempts. Ibrahim intended to sell the program on the black market. He had hoped the nonpartisan fighters in Tunisia could broker an introduction to a group with the liquid capital to purchase the program but ideologically opposed to both Superpowers.

With the program out of Russian hands, American and British engineers went to work, reverse engineering the device. Oliver let it slip through diplomatic channels that Ibrahim died during the raid; his body buried at sea. Russian intelligence never caught on to the fact the program was stolen by one of their top agents. The Dungeon allowed Oliver to return to the field to lead the efforts to further exploit Ibrahim's knowledge of the R&D facility responsible for the software. Particularly, Oliver sought out the programmer who developed the software and knew of other revolutionaries interested in disrupting the balance of the Cold War. With remote access to the network, the Americans stood to gain a significant strategic advantage in this world of superpowers. To capitalize on any such gain, much work would need to be done. New networks would need to be cultivated, new partnerships curated. In this world, time moves too fast to enjoy the fruits of success. There will always be more threats lurking in the dark over the next ridgeline in the beyond.

Chief Petty Officer Aaron D. Utsler enlisted in the Navy in 2001. His sea duty assignments include USS VICKSBURG (CG 69), Navy Expeditionary Intelligence Command, and a Special Operations Joint Task Force. His shore tours include service as the Colombia Division High Value Targets lead analyst at USSOUTHCOM, Hard Targets Branch Chief at USCENTCOM J2X, and Senior Military Instructor for the Joint Counter-Intelligence and Human Intelligence Manager's Course at the Human Intelligence - Joint Center of Excellence and Site Director for Information Warfare Training Command - San Diego Site Fort Huachuca. Chief Utsler is a graduate of Saint Leo University with a Bachelor of Arts in Religious Studies (cum laude), and is the recipient of numerous personal and unit awards. Find him on LinkedIn at [linkedin.com/in/aaron-utsler-8bb6b71b0](https://www.linkedin.com/in/aaron-utsler-8bb6b71b0) or follow him on Twitter @AaronUtsler.

Share this:

- [Email](#)
- [Tweet](#)
- 
- [Print](#)
- [WhatsApp](#)