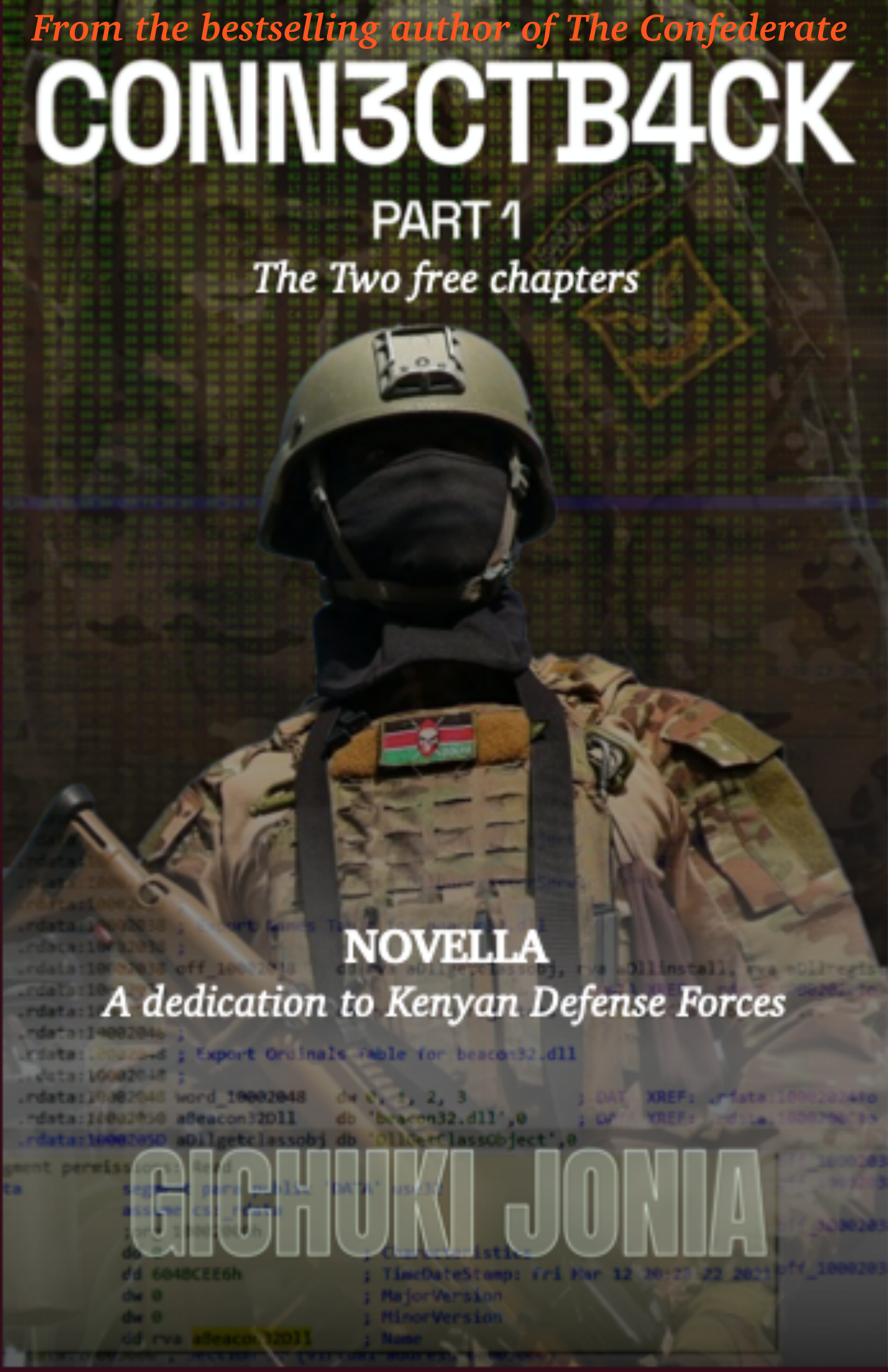
From the bestselling author of The Confederate

CONN3CTB4CK

PART 1

The Two free chapters



NOVELLA

A dedication to Kenyan Defense Forces

GICHUKI JONIA

C0NN3CT B4CK : THE OJT

PART ONE

by

GICHUKI JONIA

“The real cyber war, is for talent.” — Andrew Thompson

This is a work of fiction and any resemblance to actual events or persons, living or dead is entirely coincidental. There are some exceptions of some specific individuals like the Presidencies, Cabinets Secretaries, Heads of Intelligence Agencies, to retain authenticity of the story and geopolitics.

The materials within this novel have not been reviewed for classification.

The book is edited by : Coach Elevate Consultants

Cover design by : Khrystyna Liubynska

C0nn3ct B4ck : The OJT
is a Novella
an ARK CYBER Series One
Version 0.53 EPUB
SECOND EDITION

https://chuksjonia.com/blog.html

Dearest reader,

In my first book, The Confederate, I tried to hold back so that everyone got introduced to the world of cyber. In this new series, I decided to dip you directly into the world of Intelligence agencies, Military services and Cyber operations. It's my hope that you are going to enjoy the series and learn the goodies of cyber.

My Best,
./Chucks

BOOK ACRONYMS

2IC - Second In Command
AAR - After Action Report
ADCON - Administrative Control
ADS - Alternate Data Streams
AK - Automatic Kalashnikov
AFRICOM - Africa Command
AFT - African Financial Threats
AL QAEDA - The Base terror group
AMSI - Anti-malware Scan Interface
AMBO - Ambulance
APEX - Adaptive Planning and Execution
APK - Android Package Kit
AO - Area of Operation
AOR - Area of Responsibility
API - Application Programming Interface
APT - Advanced Persistence Threat
ASCII - American Standard Code for Information Interchange
ASM - Assembly Language
ATAKs - Android Tactical Assault Kits
ATPU - Anti Terrorism Police Unit
AU - African Union
AV - AntiVirus
BRIG - Brigadier
CAS - Chief Administrative Secretary
CAS - Close Air Support
CASEVAC - Casualty Evacuation
C2 - Command and Control
CCO - Counter Cyber Operation
CCTV - Closed Circuit Television
CDOC - Cyber Defense Operations Center
CFOB - Cyber Forward Operation’s Base
CLP - Covert Listening Post
CMOF - Cyber Mission Operations Force
CNA - Computer Network Attack
CND - Computer Network Defense
CNE - Computer Network Exploitation

CNO - Computer Network Operations
COA - Course of Action
COL - Colonel
COM - Component Object Model
COMM - Communication
CONOP - Concept of Operation
CONPLAN - Contingency Plan
CAP - Captain aka Cap
CR - Cyber Ranges
CRP - Combat Readiness Percentage
CS - Cabinet Secretary
CSOF - Cyber Special Operations Force
CT - Counter Terrorism
CTF - Capture The Flag
CTI - Cyber Threat Intelligence
CTR - Close Target Recon
CQB - Close Quarters Battle
DET - Defensive Evasion Tactic
DIA - Defense Intelligence Academy
DIE - Detect It Easy
DCI - Directorate of Criminal Investigation
DFIR - Digital Forensics & Incidence Response
DLL - Dynamic Link Library
DllMain - Dynamic Link Library Main
DMI - Directorate of Military Intelligence
DoD - Department of Defense
DOS - Disk Operating System
DRC - Democratic Republic of the Congo
DUSTWUN - Duty Status Whereabouts Unknown
DZ - Drop Zone
EAT - Export Address Table
EDR - Endpoint Detection and Response
E&E - Emergency and Evacuation
EKIA - Enemy Killed In Action
ENDF - Ethiopian National Defense Force
EOD - Explosive Ordinance Disposal
EPP - Endpoint Protection Platform
ESP - Extra Sensory Perception
ETG - Ethiopian-Airlines Group
ETW - Event Tracing for Windows
EW - Electronic Warfare
FACIALREC - Facial Recognition Software
FIN Groups - Financial Group
FRAGORD - Fragmentary Order
FRS - Foreign Resource Service (Mostly Intel and Foreign)

GWOT - Global War On Terror
GEN - General
GISO - Government Information Security Office
HAHO - High Altitude High Opening
HUMINT - Human Intelligence
HUTS - Hostages, Unknowns, Terrorists, Shooters
HVT - High Value Target
IAO - Initial Access Operations
IAT - Import Address Table
IC - Intelligence Community
ICT - Information Communication Technology
IDE - Integrated Development Environment
IDF - Israeli Defense Forces
IEBC - Independent Electoral and Boundaries Commission
IMINT - Imagery Intelligence
IMT&R - Information Maneuver Training and Readiness
INT3 - One byte instruction defined for use by debuggers
IOC - Indicators Of Compromise
IRGC - Islamic Revolutionary Guard Corps
ISCAP - Islamic State Central African Province
ISIL - Islamic State of Iraq and the Levant
ISIS - Islamic State of Iraq and Syria
ISR - Intelligence, Surveillance and Reconnaissance
IWR - Information Warfare Range
KIA - Killed In Action
KDF - Kenya Defence Forces
KENSI - Kenya National Security & Intelligence
KQ - Kenya Airways
LDR - Loader
LOE - Lines of Effort
LRS - Long Range Surveillance Battalion of the KDF’s Special Warfare
LT - Lieutenant
MAM - Military Aged Male
M23 - March 23 Movement
MCT - Movement to Contact
MDMP - Military Decision Making Process
MET - Mission Essential Task
MLCOA - Most Likely Course of Action
MOD - Ministry of Defence
MOTW - Mark of The Web
MOSSAD - Hebrew for, Central Institute for Intelligence and Special Operations
MSDBG aka MSWdbg - Microsoft Windows Debugger
MSDN - Microsoft Software Development Network

MZ - A PE header that represents ms-dos header, on e_magic also known as 5A4D
NATO - North Atlantic Treaty Organization
ND - No Daylight
NDA - Non Disclosure Agreement
NC3 - National Cyber Command Center
NIS - National Intelligence Service (Kenya)
NISS - National Intelligence and Security Service (Ethiopia)
NOC - Non Official Cover
NSC - National Security Council
NTAPI - Native API
NVG - Night Vision Goggles
OCO - Offensive Cyberspace Operations
OIC - Officer In Charge
OJT - On The Job Training
OP - Operation
OP1 - Observation Post 1
OPE - Operational Preparation of the Environment
OPORD - Operation Order
OPSEC - Operational Security
OTD - Offensive Tooling Discovery
OTDA - Offensive Tooling Discovery and Analysis
PE - Portable Executable
PEB - Process Environment Block
PID - Process Identification
PMC - Private Military Company
PPTX - PowerPoint Presentation in Open XML format
POP - Post Office Protocol
PS - Permanent Secretary
PSP - Personal Security Products
QRF - Quick Reaction Force
RDS - Rapid Deployment Squadron
ROE - Rules of Engagement
RECCE - General Service Reconnaissance (RECCE) Squad Company
RnD - Research and Development
RTB - Return To Base
RVA - Relative Virtual Address
SCI - Sensitive Compartmented Information
SCIF - Sensitive Compartmented Information Facility
SDL - Secure Development Lifecycle
SDR - Surveillance Detection Route
SFTP - Secure File Transfer Protocol
SGT - Sergeant
SIGINT - Signals Intelligence

SITTEMP - Enemy Situation Template
SITREP - Situation Report
SMTP - Simple Mail Transfer Protocol
SOC - Security Operations Center
SOCOM - Special Operations Command
SOG - Special Operations Group
SOM - Scheme of Maneuver
SOMI - School Of Military Intelligence
SOP - Standard Operating Procedure
SOR - Special Operations Regiment
SUV - Sport Utility Vehicle
SSE - Sensitive Site Exploitation
SVD - Snaiperskaya Vintovka Dragunova (Dragunov sniper rifle)
SVEST - Suicide Vest
SVR - Russian Foreign Intelligence Service
SWCADG - Special Warfare Combat Application Development Group
TDF - Tigray Defense Forces
TIC - Troops In Contact
TOC - Tactical Operations Center
TOX - Messaging App from https://tox.chat
TPD -Target Package Development
TPLF - Tigray People's Liberation Front
TTP - Tactics Techniques & Procedures
TS - Top Secret
UAC - User Account Control
UAV - Unmanned Aerial Vehicle
UC - Under Cover
UN - United Nations
VPN - Virtual Private Network
VBA - Visual Basic for Applications
VBS - Visual Basic Script
VS - Visual Studio
VSTO - Visual Studio Tools for Office
WARNORD - Warning Order
WFF - War Fighting Function
WinMain - Windows Main entry
WINAPI - Windows API
Xdbg - Opensource debugger
XLL - Excel add-in-file Link Library

CHAPTER ONE

LATE OCTOBER 2021

Brigadier Thuo plopped on the mild beige couch of the Kenyan Ambassador's office in Addis Ababa, after going through the last WhatsApp texts he got from Gebre Kebede. He had saved the phone number as Chematstone because that was his codename, and also because of operational security. He had never called him but Gebre's handler had. Gebre was one of his agents from Tigray before the conflict started. Lieutenant Nyalita was his recruiter and handler. He was the last operator to talk to him at the international's departure lane for international flights out of Addis Ababa's Bole International Airport. It was meant to be a simple bag exchange and Lieutenant Nyalita would walk through the parking lot and back to the departure's waiting area. The developed COA that was documented and cleared before the operation indicated that the exchange would be more effective inside the airport's building. Since it was a denied area operation, it would require Gebre to obtain a ticket for access to the departure floor. Given how the asset was papered, there would be no reason to think the operation was compromised.

The DMI advisors had also argued that the brush-pass goes through the parking lot for the exchange to save money. For them, it was just Excel docs and balance sheets.

It had worked seamlessly until Lieutenant Nyalita was met with a hail of bullets as he threaded through the car park.

The Brigadier had taken the first flight out of Nairobi. He had used his diplomatic passport as an officer of the Foreign Affair's mission in Addis Ababa. The Ambassador had to act quickly to support his travel and documentation. Someone had to go and collect Lieutenant Nyalita's body from the morgue. It was proving to be unsuccessful because the Ethiopian law enforcement agencies claimed they needed more time to investigate. When Madam Ambassador had asked for a copy of the CCTV at the airport, the officers had explained that the cameras stopped working one hour before the gunfight. The shell-casings showed it was a Mac-10. The commotion illustrated that it was a robbery. The erratic shots from several other goons showed it was an amateur shootout.

But Brigadier Thuo believed a state actor was behind it. The amateur hour was just deception.

Lieutenant Nyalita had just come from a harder and longer undercover mission in the DRC. It was all, NOC. He had not even seen his family for almost a year. To him, this was just a simple exchange. He had told the Brigadier how front sight focused he was to clear this mission fast and get back home, for a longer Nov-Dec holiday. December was just around the corner.

Nyalita had laughed at their last meeting inside the Hurlingham DOD's SCIF, "Easy in, easy out, sir. Just an exchange, sir. Zero footprint."

He was dedicated to taking out terrorists off this earth.

He had not fully completed his DRC operations' AARs.

He had taken a flight out the next day.

He had texted the asset on WhatsApp for the brush-off.

DOD officials working for the Brigadier had expressed that the Lieutenant was rushed into this.

The DMI advisors were against him taking the mission without a psychological test.

This was because he was embedded undercover on a mission inside an ISCAP's killer squad. This squad was deep in the DRC's main ISCAP's function which he disrupted amicably, thus affecting the amassing of M23 operations. He had conveyed to the brass during a secure online brief that the tactics employed by M23 appeared to be predominantly imported. Lieutenant Nyalita had lost numerous informers prior to the penetration of the ISCAP killer unit that he was targeting, as well as encountering significant losses within the M23 strongholds. They had suggested that he could have some form of PTS, or other issues that related to Hero Syndrome/Messiah complex that should be addressed before undertaking any further missions on meatspace.

Brigadier Thuo had contemplated that the Lieutenant was one hundred percent to go. He'd said that his operator had ran operations in much more difficult and non-permissive environments.

And Addis Ababa wasn’t one of them.

The Major General in charge of Directorate of Military Intelligence had agreed to sign off and green-light actions-on. Simple operations were the ones that worried him. He had pulled the Brigadier out of the SCIF and rapid-fired a lot of questions. He had told Brigadier Thuo, “This operation feels like it's full of landmines, but I agree with you. However, in any way anything happens though, during this mission, you will carry the cross. By yourself. On yourself. Agreed?”

The Brigadier had to consent to the new arrangement with an exception of the follow-ons. The General was overwhelmed by the politics. Like always, the decisions on political issues outlasted the safety of his men. The Brigadier had experienced combat. The General had forgotten how to use a firearm. He had never known what it meant to send men into the fire. But over the years though, the Brigadier had learnt through experience never to break the top rules in DoD. The most important one being: Never make your boss look irrelevant.

Yesterday, Lieutenant Nyalita died alone.

He had no backup.

He had no over-watch.

He always had a team shadowing him even when he was UC or NOC. And that was throughout his career.

Chematstone was nowhere to be found.

Brigadier and his teams had zero comms on him.

No one was embedded on Chematstone’s operation to even take the temperature inside Addis Ababa. Using cyber, someone had managed to disable the airport cameras for over an hour during the gunfight.

It was a complete mission failure that had turned into a bilateral disaster between Ethiopia and Kenya. The Brigadier had no choice but to press forward because this was not the type of mission where operators take casualties.

Normally, if gunfire goes off during a spy mission, then something has gone incredibly wrong.

The Brigadier had requested for more FRS resources within East Africa to support in the recovery mission. Statehouse and Office of the President were against it. He knew the Kenyan Ambassador in Ethiopia was a former NIS supervisor. He knew she had assets inside Bole International airport and inside Immigration offices, and their ICT personnel. She was good in HUMINT especially recruitment of agents. She had created a web of assets around the world.

He had asked her for help. She had asked her asset in Ethiopia to find a way to recover the footage from the Bole’s Disaster

Recovery site. He had access. His intervention to copy footage directly from Disaster Recovery data center would totally burn him. He was spying on his government for the Kenyans. He was paid in US dollars. He was delivering the hard drive to her. He had to be extracted out of Ethiopia after the delivery. Brigadier was patiently waiting on the couch in her office on upper floors of the Kenyan embassy, gazing at vehicles speed outside Comoros Street.

The door opened and he glanced back behind the sofa and saw Ambassador Priscilla Kiarie standing with her hands akimbo. She had a hard drive on her left palm. She still had yesterday’s clothes on but her hair was neatly held back.

“Priscilla,” Brigadier stood up. “You were able to get it?”

“Told you.” She answered nervously. “But we had to get our asset to a safe house. He was already made. He came through for us you know. We are moving him out of the country in two nights. Ethiopians are merciless because of what they don’t want us to see up north. If they catch up with him, he will suffer for a few weeks in a hole.”

Brigadier Thuo was well-acquainted with the harsh reality of espionage, where agents faced torture under certain regimes.

She added. “Then they will totally torture him before they kill him.”

“I’m sorry.” He apologized. “He should get out of country as soon possible. They are turning the heat up because of Tigray.”

“Let’s look at what we have here first.” She allowed the door to swing shut behind her as she strolled toward her desk. “After this I am heading straight home.”

“As will I.” The Brigadier asked. “I hope the NISS and Federal police are not all over you these days?”

“Why wouldn’t they be? I catch their counter intel chaps and whatnot all the time.” Ambassador Priscilla laughed. Brigadier watched her as she worked the machine. She tapped the keyboard to get the iMac up. She moved the mouse to the password box. She typed her credentials.

“You are their top HVT?” The Brigadier joked back. “Top spook.”

Priscilla gave him a smile, “As always. NISS guys are good. They are trained by Mossad you know. But as a woman, they always think I am inferior. They underestimate me all the time in the field.” She looked up to him as he approached the desk. “And you are getting older and younger at the same time Brigadier.”

“Yes?” He couldn't hide his grin too, “Like fine wine my dear.”

“Yes sir. As they say, wine is fine and whiskey is quicker.” She gave a chuckle and hooked in the two TB hard drive. “The files are on RAW format from the six cameras. Each file is around a hundred GB with two hours' footage. They should upgrade the tech at the airport."

"Ha! Okay." He laughed because he didn't understand most of what she said.

"So your team will need to get the exact timelines." She clicked on the mounted hard drive. The rainbow wheel spun, and the finder popped up.

"You should have a backup." The Brigadier asked, "Can you make one?"

"I don't think I have space." Priscilla's expression pinched.

The Brigadier could see she was a bit reluctant on the backup idea because she was running on fumes.

Priscilla leaned her elbows in as she hovered the mouse on 'About This Mac' tab. She told him, "But, uh, lemme check."

"Okay." The Brigadier pulled a chair next to her. "This ICT and Cyber stuff is for the young ones. My daughter had to give me lessons on Skype, so that we can talk when she is away."

"We are still young Bwana Brigadier." She said and clicked storage. "I've some space. I need around six thirty GB. It's there."

"Let's see what we have first."

Ambassador Priscilla rolled the mouse back to the finder. She clicked on the hard drive and opened a folder named FootageNov. She tapped her finger on the mouse and then clicked open the folder. The files were there but they were not identifiable. "They need to be converted."

"Can you convert them?" The Brigadier tsked his tongue.

"I can try VLC." Her shoulders tensed, a subtle indication that the need to explain weighed upon her. "VLC picks up several streams of video. The conversion of these files will help a lot but it will take time. And I think your flight is this evening."

"I have five to six hours to kill I guess. Does NISS have counter intel team outside our gates?" He pointed outside the big embassy windows. "I didn't see any cars parked over there. They should be busy because of Tig."

She laughed. "They are across the street. On the other side. They have upped their efforts on us you know. The Ugandans, Egyptians and Americans too."

Brigadier Thuo strained his eyes. He attempted to discern any of their cars, but the passage of time had taken its toll on his vision.

Priscilla opened VLC from the dock. "I'm sure they know who you are and have an idea what we could be doing over here. There is no need for SDR though. Just go straight to the airport. Okay?"

Brigadier Thuo nodded involuntarily.

She remarked. “Trying to lose them on the other hand might cause more drama. We don’t need that.”

“Roger that.”

She dropped the first file on the VLC window. The rainbow wheel came back up again. “Huge files, wah!”

The Brigadier willed to ask more even if he knew what she was doing. “You did Computer Science?”

“Yes I had to.” She leaned forward again when the video came up. “Everything was moved to computers at the service.”

The Brigadier tried the same.

Priscilla moved the screen for him. She clicked play and pulled the timeline bar further down up to 1155hrs, which was almost 50 minutes on VLC. The screen showed the outside of Bole Airport, black and white. The footage had no sound. “There. Three white males.”

Two men had picked up Lieutenant Nyalita’s trail.

They were watching him at the arrivals.

They had baseball caps on.

They were talking on earpieces.

“Professionals.” She pointed at the screen. “They didn't engage until he brushed with our asset. Have you heard from Chematstone?”

“Negative. He is dark.” He sank back to the chair and rubbed his knees. “If this is NISS, then this an escalation.”

She stated the obvious. “They could be protecting an operation.”

“I think so too. We will keep looking for Chematstone just in case. We could also have a leak at the Directorate.” The Brigadier fumed, “I am too old for this crap.”

"Probably. I might say. LT was burned before he even set foot in Addis.” She said. “We do that to them too but —”

“Yes.” He allowed it. “If there is a leak, then it's someone close to the office. Someone with operational details.”

She craned her neck to look up at him.

“But.” He felt his eyes narrow. He let his gaze find hers. “But, we don’t kill each other. It's just espionage between our nations.”

“Well.” She said, letting out a long breath. “It’s the business we are in Bwana Brigadier.” She pushed back on her chair. “Alright— Okay, soooo — let’s copy all these files.” She closed the VLC. “You will need to have all conversions go into MP4 formats. You should start around fifty-five dot thirty-two. Until after gunfire.”

“Thank you.” Brigadier Thuo strained to commit the location and time to memory. “Let me call Captain Mwangangi. He needs to have his team ready for these video files.”

“Different camera angles. Remember that sir.” She insisted. “The files are too huge. They can’t be sent over email.”

“Yes they can’t.” He agreed pulling his phone out of his inner jacket pocket. “I will walk with it at the airport. I hope you still have the diplomatic pouches?”

“Yes, sir.” She answered as she turned to the safe behind her. She punched her code, yanked it open and pulled a diplomatic patch for Brigadier’s laptop bag. She then rummaged through some folders and took another classification hard drive sticker. There was also a red diplomatic pouch. “Here you go.”

CHAPTER TWO

The Brigadier walked out from the outer upper stairs of the Embassy with two men ahead of him. He was the tallest, and he looked like the largest peak from Mountain Kenya, during the morning hours of Kikuyu-land-dews.

He had his weird old hat on and a laptop bag slinging from his left shoulder. One of the men up front was the driver and the other a body-man. The two men had received strict instructions from the Ambassador due to the volatility of the situation: 'Make sure the young man gets into his plane.'

They always laughed at how she called older military men, 'young men.'

With her background in the intelligence community, she already knew how easily a closely guarded operation can be carefully executed and could then end up veering off course in a matter of seconds.

Getting the hard drive to Nairobi was a sensitive operation. If NISS knew they had the footage or any other opposing party that was involved had wind of it, getting the Brigadier out of the way was an op that the adversary would execute in a heartbeat. The vehicle he was in was armored. Both men in front were armed. Two more automatic M4 carbines were below their seats. Engaging them en route would have causalities on both sides, especially if this entity tried to mix it up.

Knowing Ethiopians, they totally would.

They are known cousins of Jews and the Jewish community believes in the security of their state. This somehow was inherited by the Ethiopians security services over the years.

The SUV turned into Comoros street from the Embassy exit gate.

The Brigadier immediately spotted the two cars from NISS pull out front and slow down waiting for their SUV to pass.

The driver mumbled. "Here we go. They never wait. They luck patience. It was not instilled into their intelligence officers."

“It’s like they are escorting us.” The guard whispered as he pulled his weapon from the left side of the jacket. He sat upright. “They can’t do anything here.”

“No SDR.” The Brigadier slipped into the discussion in Swahili. “No SDR or any evasion whatsoever gentlemen. I repeat, no SDR gentlemen. Just get to Ring Road and head to the airport. We don’t need any hubbubs.”

“Copy that sir.” The driver agreed with him. The guard nodded back. He rolled his side window halfway to have a clear sight of the side-view mirrors.

The Brigadier held his laptop bag tight. He pressed on the side of the diplomatic pouch just to make sure everything was still settled in there. His subconscious was testing him. It felt like NISS operatives, would snatch it by osmosis. Grab the pouch through the cars, as if EW had osmosis. He still didn’t understand Electronic Warfare nor Cyber Warfare. Not many in the leadership understood Information Operations or the domain either.

The two NISS vehicles shadowed and changed lanes with the SUV, through the highways and to the Airport road. The Brigadier made a call to the Captain Mwangangi. He didn’t answer until the fifth ring. The Captain was currently assigned to Moran Cyber Center. It was an upcoming unit which was getting a longer and comprehensive cyber ops training at the Defense Intelligence Academy. The institute was formerly known as SOMI, that is School of Military Intelligence.

The Captain was now waiting to pull all the videos and convert them into MP4s. This would make it easier to feed them to the teamservers and analyze them for a better understanding of the shooting. All they needed was to check how the shooter got to pick Chematstone and the Lieutenant from the crowd.

Were they following the asset?

Were they on to the Lieutenant after he landed or before he had?

Or was the attack planned from the time the Lieutenant left DRC?

Was his operations at DRC compromised?

Because all this was not coincidental. If a shootout happened during an intelligence operation, it was because someone somewhere fucked up.

The SUV drove up to the security ramps and into the entrances of the Bole International Airport as did the two opposition vehicles that were following. They immediately collapsed toward them. The Brigadier could see that the occupants of the nearest vehicle were three and the man at the back had his radio up.

Their driver had tactical wrap-on shades and his view blocked by the car's roof.

It was as if OPSEC was not a priority for the team. It was more like impact over cover.

The Brigadier's heart pounded so hard that he was sure the opposition could hear it.

The bodyguard asked the driver, "They didn't try anything. Will they push the envelope inside?"

"I doubt it. But be vigilant." The Brigadier turned to the rear window and glanced back at the cars. He clutched the pouch in his lap.

The guard shifted on his seat to get his handgun back into its concealed holster.

"They can't." Brigadier Thuo's expression did not change. He added, "But, they might follow me around inside the airport. They have no idea what I have. But they might try to take a peek."

The driver dropped a nod and the bodyguard said. "Copy that, sir. I will walk you to the gates."

The bodyguard jumped out after the driver parked the car near the entrances to Ethiopian Airline advertisement billboards. He looked over his shoulder to check if NISS cars had stopped too. The nearest was the old van hanging back a few meters away. Dark exhaust trailed from its tailpipe. He walked around to the other side of the SUV. The Brigadier watched him clock two white athletic ladies in shorts, carrying large duffel bags. They jumped aside as the door flew open.

The Brigadier shouldered the door out and groaned. "This is old age, Kariuki." He then said the same in Swahili as the bodyguard chuckled back another Swahili joke about keeping their women happy.

"When were you last home?" The Brigadier asked Kariuki.

"Seven to eight months." He answered. "I am rotating back this January just after Christmas. I will be home during the coming elections."

"Who do you think will win?" The Brigadier asked laughing. He pressed his hand to his chest.

"Obviously the Hustler. Even Ethiopians love him here."

Both men ruefully chuckled as they walked into the airport door for the check-in.

Kariuki noted. "It's the story of an underdog. It touches everyone at heart."

On arriving at the gate-check, the Brigadier turned to him. "I know you can't go because of your weapon. But good luck with everything young man."

“Yes sir.” Two more Caucasian women in glasses and large duffels bumped into the bodyguard, while chatting and giggling.

Kariuki shrugged with the same amusement as he glanced at their legs.

The Brigadier pulled him back to their conversation. He asked in Swahili. “Good luck?”

Kariuki looked up at the massive security screening area. He told Brigadier Thuo. “You need more luck than me sir. Travel safe.”

They shook hands.

“Thank you young man. See you in Nairobi next year.” The Brigadier muttered as he stepped in for screening. He smiled at the gate-attendee. He had that strained weary smile of an old traveling man.

The attendee grinned back. “A’ salaam.”

The European women were chatting about Kenya behind him. They were involuntarily bumping into him. They were in a hurry. The duffel-bags were stacked between them. He dropped his belt and shoes on one of the buckets.

Both women paused and laughed at a joke that the Brigadier couldn't understand due to their Slavic accents. When he set his bag on the screening machine, they immediately rowed theirs too next to his like it was a contest. That somehow surprised the Brigadier but he didn’t think much of it.

The two ladies were still laughing and had switched from English to some Eastern European language. By the time he moved to the other side, his laptop bag was between the four large bags that seemed like they had packed bricks in them.

“Good Lord,” he breathed almost a prayer as he reached for his bag. He murmured in Swahili. “Hope they didn’t break my stuff.”

One of the girls growled at him then playfully smiled.

The Brigadier paused and watched as more passengers funneled through the gates. Several had already started unpacking their bags and removing their shoes.

He nodded at her and lifted the bag wondering why the security didn't check the contents of the laptop bag. The diplomatic patch caught his eye. Brigadier Thuo was an old school spy, and use of technology for IMINT or SIGINT sometimes flew over his head.

He slowly picked up his shoes and then his belt. His back popped. He stretched and took a nearby chair. The Caucasian ladies were cleared almost immediately and they walked past him again.

A cleaner waltzed behind them with a clean cut khaki uniform.

Someone was playing Swahili Nation’s music down the hall.

The Brigadier tried to read the cleaner's uniform so that he could avoid the two scantily dressed Europeans. It showed that he worked for ETG Cleaning Services. He decided to follow him through to the concourse and to the Addis Ababa's duty free section.

Brigadier Thuo sat near the Ethiopian Airline advertisement board. His eyes and ears were more alert. He could hear the familiar announcement and warnings of a flight about to lock its gates. And then that ding that is followed by a slow voice on the next flights.

The international terminal was way larger than JKIA's. Or maybe not. There were restaurants, fast food cafes, bookshops and the occasional fashion stores. The airport was not crowded, but the ladies he walked with were a few meters away on the other side of the open floor. They seemed innocent but as an old school spy, anyone could be hostile. He checked his bag, and confirmed the hard drive was safe. Someone dropped their traveling suitcase, then picked it and cursed in Kinyarwanda. A group of Kenya Airways pilots and flight attendants hurried by. Several African couples were on the left and another old couple was walking towards Alfarag, where the Duty Free shop was. The Cafe Satellite Restaurant was opposite with a full display of all types of pastry. The Brigadier felt his stomach grumble. He saw the same two European ladies near an escalator far up. He decided to get some tea while he waited for his flight. He slowly picked himself up and walked toward the restaurant. He stepped in and almost collided with a traveler glued on her screen reading an email aloud.

The Brigadier crawled into one of the chairs that faced the outer floor.

The two ladies with their duffel bags also walked in and smiled at him. They both pointed at the wall behind him and read, their voices resonating with the words like a chorus. "Authentic Taste of Ethiopia since 1922."

The Brigadier turned his back to check and then one of the ladies approached him.

She said. "You were at the entrance with us."

Her accent was Slavic, like she was Russian, Polish or Lithuanian.

The Brigadier smiled back at her. He didn't reply.

She held out her hand to the Brigadier. "Marta."

Coffee or milkshake gushed somewhere, immediately easing the tension he felt. He was looking at her legs just like Kariuki did.

“How are you?” He shook her hand hoping she wasn’t a spy. Just another lost tourist. Lost in the East African jungle as they all thought.

“Your name?” She asked, flirting. Her lips twisted into a smile. She whispered, “I’m Marta.” She pulled the word, “M-a-r-t-a.”

“Oh.” The Brigadier had not caught the Slavic name earlier. He lied. “Joseph. Call me Joe.”

The other lady was joining them.

Marta said. “That’s Anya. We are heading to Nairobi. Safari, yes!”

Anya lifted her arm up into a fist. “Yes!”

“I am heading there too.” Brigadier Thuo replied glancing over onto a shop across the hall that had traditional African outfits. He wondered for a moment if he should leave and check out the shop instead.

“Can I put my bag next to yours?” She asked as Anya joined them. “You have to order the tea at the counter.”

“I can order for all us.” Anya said as she set her duffel next to Brigadier’s bag. It cracked like rocks. She giggled and then asked Marta. “Chai tea?”

“Khorosho. Ja bud kofe?” Marta instantly and subtly shifted the topic. “Maasai Mara or Naivasha?”

The Brigadier looked at the counter for guidance. He wanted to get out of this, whatever it was. Shopping for the outfits across the hall felt better.

Anya was already ordering tea and coffee for them. She waved over and sharply asked. “Queen cakes?”

The Brigadier beamed and nodded.

Marta sat down and leaned forward on the table, her chest bazooming together. That’s when the Brigadier felt the incoming sexpionage. He said hello in the little Russian he knew. “Zidiravustivuyi.”

“Haha …” Her laugh sounded forced.

Brigadier Thuo knew little to no Russian, but that was the only longer Russian phrase he had picked up from old spy movies, along with other frequently used words like 'da' and 'neyt' in their sentences. Nighttime TCM had done him no justice.

“Zdrastvui.” Marta put her hands on either side of her cheeks cupping her chin. She was totally flirting with him.

Brigadier Thuo’s hand went to his chest. His phone was secure and turned off.

He glanced at his bag. It was safe, between the two big duffel bags on the other chair.

He guessed; *This is SVR.* The Brigadier had never interacted with Russian Foreign Intelligence service before. But he had learnt of the Swallows and Sparrows from friends of friends. Mostly around western intelligence community circles. He muttered to himself, “Two can play this game.”

She smiled at his uneasiness.

Brigadier Thuo’s ESP antenna went high up. The young master and the operator from the days of counter espionage against Ugandans, was now back online.

CHAPTER THREE

Training cyber operations was essential to KDF.

The third Secure Ark Cyber's training was going on well for the DMI classes at the Garrison. The current students, officers and servicemen had to be sorted out from a large number of candidates. They had already gone through the first inceptive class that operators should have earlier; before joining tactical CNO order.

It was now the beginning of the third month, for the ongoing Information Operations and Maneuver training, also commonly known as Information Maneuver Training and Readiness, IMT&R.

They had practiced several languages with their main trainer, Richard Mbatha of Secure Ark Cyber LTD. Moula Bukstein, his boss only showed up on the second month during Initial access operations class. When she explained ADS, introduced structures like WIN32_FIND_STREAM_DATA, and discussed an API known as GetVolumeInformation, along with explanations of Wipers and Ransomware, the class erupted with rounds of questions. It seemed as if they all had a strong desire to learn CNA rather than CNE.

Moula had the task of adapting a two-day class on Ransomware and Wiper discussions in order to train DMI students in the development of XLLs, as well as creating a dropper using C/C++, with a particular emphasis on evasion techniques. This session was specifically designed as an introduction to initial access operations, catering to her extended schedule.

They had learnt some effective AMSI and ETW maneuvers that were required during dropper operations for effective initial access tactics and how to document them for CONOPs.

Captain Mwangangi was the OIC in class throughout since Major Ngure had not showed up. He had to follow up with all students to see if they understood what Richard, the lead trainer, showcased in class. Some of them would get lost with the modern military wording and acronyms. Some would get off-track due to the Windows API naming convention. But the Colonel in charge of Cyber initiatives had told them on the first day that they had to work hard and understand what they were being trained on. This was because the enemy was learning these tactics too, and the KDF was supposed to master and prosecute better against these upcoming adversaries. The team was meant to be the tip of the spear in the modern warfare space, and of course operate with reference to the Information domain proficiency and readiness.

This morning the team was now turning in from Introduction to Computer Network Operations class and into Tactical Developmental Operations.

Besides, Introduction to Computer Network Operations had several subjects that all the students had to get a grip of.

That content had taken them three months in class to master. Richard and Moula had told them that there were no shortcuts. Cyber was always like specops. They all required longer trainings with emulations and simulations.

It's like a training or a class that never stopped.

Of course Cyber range and Information Warfare Ranges, IWRs were essential. The students were required to show case their CRP, (Combat Readiness Percentage) during live fire on the range. Their classes rolled up as:

Introduction to CNO and Cyber Weaponry.

Introduction to major Programming languages for use in class.

IDEs and their corresponding languages.

A sneak into tools used by AFTs, FIN groups and the sampling of APTs weaponry.

A deeper look at APT Ops and Tactics, Techniques and Procedures. By this sub-subject, the students had started to worry they would never be in a position to understand Assembly or even C/C++ coding for CNO tooling. Some said they preferred Python. But Moula had specified that such high level languages should only be used on the Listening Post side, or on the Command and Control servers, and if required on the Team Servers. If diversity was needed especially on data analytics, because cyber collection usually has heavy data streams and large data sets, especially due to collection at rest; then at all costs it was important to make sense of all SIGINT data collected in bulk.

Hence Team Servers.

"High level languages should never be on the active endpoint side." She had stressed during class. "Unless OPSEC is a major after thought, no cyber leadership or CNO planners should allow that."

The training went on into other sub-subjects like:

Injection Techniques.

Anti-Analysis Techniques.

How to tool like someone’s else APT.

OCO to support Computer Network Operations and military meatspace operations.

At this point the students were approaching the third month of hardcore Information Maneuver classes. They were okay with how long the classes were, until they had indirectly requested for a few days off to cool their heels.

After one week of break. OCO to Support Computer Network Operations was the next sub-subject to engulf into. The break was worthwhile, because this morning all the students were front sight focused.

Richard Mbatha turned on the PPTx on the big screen. “I hope we are all ready and set to continue.”

Captain Mwangangi glanced behind him. He nodded to everyone and then turned back for the training to commence. “Good to go sir. Charlie mike.“

“Copy that Captain.” Richard had turned his body to the big screen. “Let’s dig in ladies.”

The first image on the screen had the next class illustrated as class 4.0. OCO was now shown in detail as the ‘Offensive CyberSpace Operations.’

Richard said. “With Moula, you did the dropper when she was here. She had showed you the detailed representation, on hiding that PE as it was getting dropped by the Dropper. Straight onto disk and then rearranged into a DLL. That’s right, from a bin file brought in as a buffer. So gentlemen, that’s just an example for initial access operations. From now on we will refer to that as IAO. I know she didn’t show you the definite measures that an operator will need to look into when bringing such a weapon to bear during operations. Remember we have to take note of Pre-execution stuff; that’s the first part of the measures we require during IAO. But the only evasion shown on that dropper class was bypassing the Mark of the Web which I don’t think Moula went into full details. I would like to do that later.”

The students were silent because at some point asking more questions always stretched the class further. They also knew that the trainers would always drum them up on getting their private study's hours in.

Richard had the class videos loaded on a portal for evening and break-out sessions. That was like clockwork immediately the sessions were done. They still appreciated the trainers’ thoroughness. Richard turned from the screen to them.

The first hand that came up was from Senior Sergeant Duncan. “I think we got it —”

The man always sounded like a young Steve Harvey. Moula was right. He was the Kenyan version of Harvey's swag.

"Was it shown by Moula?" Richard asked him, interjecting and walking toward the first table-rows. Although he had promised earlier he would let them finish what they wanted to ask, Richard still answered his own question. "I believe it was. Yes — And Mitre Attack does help in some way. Yes."

Nation state intelligence collection often doesn't serve the interest of infrastructure defense. Training them how to penetrate without being caught was a priority as far as initial access operations were concerned. Mark of the Web was an important study for the students and Richard had to get them to learn that essential capability. It was important for the freedom of maneuver during ops in the information domain.

Richard remembered discussions on Zone.Identifier Alternate Data Stream. This would be where a file is downloaded from the internet plus the records that showed the URL, and the referral from the page visited. He told the Senior Sergeant. "Moula explained a lot on MOTW if I remember correctly."

"We didn't get much of it sir, but at least with some studies and testings I hope that could help us big time to understand those *pathways* — or rather — as you bypass the Mark of the Web with that dropper."

"Right." Richard consented. "We will go back in detail once we understand the defense and detection tech that the adversary might use. Or let's just say, the target. That's 'cause, it's not all the time that CNO will be executed against adversaries. Sometimes it's just a tango that we need to collect intelligence from. SIGINT as we know it. Sometimes even locally or from a friendly nation. Our priority requirement during CNO is collection. Right?" He chuckled, "Right ladies?"

"Sir. Is there a way we can like revise that class from Moula's sessions?" Senior Sergeant Duncan asked, still with his hand raised and his dimples deeper. He persisted. "It would be nice to ask her back for a revision study on the class."

It was not because the training was done by a woman that made Duncan like it, or that Moula was trans (even though they didn't actually know that.) For Richard it seemed like it was something else about her. He wanted them to wake up. He quipped. "I know she be carrying."

The class laughed. They were disciplined men but they always enjoyed the occasional banter.

"Hey, nobody say I said that." Richard continued amidst the laughter because it had woken them back up. "The videos for that class are still in the portal. What I will ask you to do is, you go through them again from Friday through the weekend." He turned to walk toward his table so that he could switch over to the next PPT page. He said. "Then we can always go through those options that we did not understand."

Duncan answered. "Roger."

Richard passed the Captain's table as he nodded towards him and said, "I think that's a good plan Mwalimu Mbatha."

The Senior Sergeant agreed again and was back on his keyboard.

The trainees had been given new laptops. They had to, it was mandatory. They were expected to be the new special operators for the military in the information domain.

Each had two in front of them, one on Microsoft Windows and one on Linux. It was a recommendation as the class progressed. The Colonel in charge had been pressed by Secure Ark Cyber officials to process that in quickest time possible if he wanted his students to grab all tactics needed for special cyber warfare activities. They were supposed to be the new Special Cyber group as rumors of the Moran Cyber filled the intelligence community corridors.

Richard pulled back his chair at his desk and dropped heavily, "We are going straight to OCO class in support of CNO ops. I appreciate that we have had a good one over the few weeks on persistence operations inside a target endpoint. Yes," He chuckled lightly. "Just like the way Moula did the runkey automatically with the dropper when the bin file hit the disk. I remember there were other methodologies that you practiced with her."

The CONOPs Moula showcased had made the team realize the need to design new approaches during CNE. Breaking away from routine execution of ops and standards, often requires unique minds.

Richard took a sip of his tea. "We have also done several introductory classes that required minimal programming efforts and methods as per the commander's directive."

Richard switched to the next page from his MacBook and the PPTx rolled over on the big screen. "For us to get to OCO ops, it will be important to understand detection tech used by organizations that you may need to penetrate or have access to during CNE."

His table had three laptops. One small Linux Lenovo loaded with Microsoft Windows. The other was a big i7 laptop on his right that had Linux Mint that carried his RnD. And in front of him as he trained through the presentation was his MacBook. He said, “For us to bypass this, we need to understand normal firewalls and detection techs plus some greater understanding of AVs, or rather Anti-viruses. In CNO ops, we call them PSP or Personal Security Products.”

The students were already now glued on the screen. The new cyber terms combined with modern military lingos were still highly intriguing to the class. Richard wanted to tell them that it would get better but he was not going to lie. They would have to pull their weight and study harder. Cyber required hard work, creativity, innovation and talent.

“In a nutshell.” Richard stood up to explain, “These will include, how to make the Windows Eventlog go blind and follow it up with ETW patching. This will be important especially as we understand Sysmon and how to evade it. I’m sure you have some experience with some sysmon. Have you?”

Several sergeants at the back nodded. The Senior Sergeant didn’t and the two Lieutenants seated next to the Captain seemed to disagree on the question.

Lieutenant Arun asked. “We can have sysmon on CTFs?”

Richard followed his gaze with half irritation and half a grin. This was because as military personnel, they were supposed to know that CTFs are for high school kids and beginner college students. It was like training militaries forces with water guns and sending them to war. Richard saved the Lieutenant the explanation. “Like I said before, we are a much more mature unit, expected to perform ops. Due to that effect, we will either work Cyber ranges, or go directly to Information Warfare Ranges. No CTFs.”

The officers on the first row agreed. Lieutenant Arun was not pleased by their assessment. Most of them knew what an IWR would do for them, since they had experience planning conventional ground offensive operations in Somalia.

“Anyways, we will get to sysmon.” Richard had realized their differences, especially the lack of operational planning background and so he had to affirm his theory. “No worries. We will also learn how to make that PE you wanna execute on the target look more legit. This is important, e.g. signing it and other techniques. Also detecting what the other side is using so that you can make better and wiser decisions on follow-on weaponry. It will be important for you during decision making of a perfect planned OCO. Understanding their CND arsenal can help you prepare and evade better. That’s what we call discovering enemies WFF and SITTEMP. Their operational plan too. And that’s when we prep a MLCOA.”

The students nodded and seemed to get the issue at hand. They knew WFF was War Fighting Function and SITTEMP was another acronym for Situation Template. In the military, everyone loved their acronyms, and KDF wasn't entirely familiar with the new ones from NATO. At least they understood several adversaries would be equipped with high-tech security products if they were hiding something. What they didn't understand is how to prep an enemy Most Likely Course of Action.

Richard walked near the screen and continued. “We are trying to finish this session in the morning because it's theoretical. It's good that we hammer it when we are all sharp and you can still put up with my incredibly soft voice.” He chuckled lightly. “If we did this in the afternoon after the *Ugali* havoc, you would all be in dreamland.”

A small laughter came from the back that lit up the whole hall.

“I would understand though.” Richard laughed a little too. He pointed at the screen. “It happens. So on all that gentlemen, we can start getting into PID spoofing, and we then go to disrupting EPP network comms and if we succeed all this by end of the week, we can get the CNO Tooling class up.”

The Captain murmured. “Very interesting.”

It seemed he was glad he came to this class. Most military captains in old school African regimes never wanted to be in such settings where servicemen attended. It was almost like an unspoken rule.

But cyber was different especially in well trained cyber armies all over the world. Such that you would find even Generals attending a cadet’s class, with the young cadets learning cyber, because they knew warfare in the cyber domain needed a newer mindset.

Richard moved the PPTX page. “We will discuss a little more about sysmon, as we get to modern EDR perspective.” He scratched his jaw and continued. “It’s a traditional EDR at some point which does the normal monitoring aspect of an endpoint, though not as advanced as commercially available EDRs we are seeing nowdays.” He leaned down into his tea again. “I think even you guys should start to make sure they deliver tea for everyone. Don’t worry, we will pay if they charge us. Ha ha ha.”

The class laughed it out in unison. A cup of coffee in class would make all ideas come into the air.

“Anyway, the EDRs will inject their code into other processes that they wanna monitor, and also they do hook into some APIs, same way we will do when writing our Stage0 OPE implant, or even on our Loaders and other types of Implants. This will depend on the TTPs we choose. It’s going to be important for MET. Rather our Mission Essential Task as far as this training is concerned. It will also be important for you when you go back to research and for your studies, and— and when you look at the user-space and the kernel-space for each of your operating systems. Actually that's your homework for this weekend. I will need a one-page paper on this, 900 to 1000 words."

One of the Sergeants at the back snorted. They weren't expecting homework immediately after the first week back. The class laughed again because they knew it was a pun intended protest.

"I am sure they still need a break." The Captain threw a remark.

"I know rest is important, we will catch a break after the next week coding sessions." Richard asked, "Three days out?"

Everyone nodded. The Lieutenants too seemed to agree with the Captain's gesture.

Richard smiled and moved back to his chair. "I know this class is difficult. So those breaks are important. When you get the breaks, use them wisely. This contract to train CNO is for six months unless extended by Colonel Cyber."

"Agreed." Lieutenant Arun grinned. He was telling the Captain. "Agreed …"

"Okay gentlemen. Let's proceed." Richard sat back into his chair and switched to the fourth PPTx page that had another large text, 'EDRs.' that was in red. Color of the day. He pointed at the screen. "Endpoint Detection and Response units will run as a dedicated service on user-space, and as a driver on kernel-space. For this class, we will look at the user-space level first. Once you study this user-space from your homework, you will fully understand why. Because the EDR will be checking for some kernel stuff, network activities, processes, memory, disk usage, registry and some other system actions and events. When you study the kernel-space, I will need you to look keenly at the Kernel callback on our first endeavor since by now you know how to play with Microsoft Windows Debugger. The MSWdbg."

One of the Lieutenants, who was in-charge of timekeeping, winced at Richard specifying it's almost time for the 10 o'clock tea.

"Copy." Richard answered. "We got thirty mikes to go before tea break. So let's step into how the EDR will detect and check processes that could be hostile on an endpoint. As usual, the EDR will inject its DLL into a running PE image of the process in memory. I believe we had a class on Process Injection before. Basically, EDRs do the same and it's only that they are signed and — and the AV on the endpoint doesn't see that injection, as malicious even when it runs. So if you had a signed DLL that injects to a process, no one will be wiser. You will get your target endpoint calling back to your C2."

There was a 'whoa' at the back.

The Captain seemed surprised too.

For his sake, Richard added. "CMOF are ground remote team. Maybe stealing certificates in the field can help further the cause."

The Captain wasn't one for cliffhangers. He said. "The certs are usually under lock and key. Highly secured facilities."

"That's right." Richard scratched his chin. "Anyway, that's just a basic example. We will go deeper into it."

He didn't not address the concern. Defensive evasion during IAO was a convenient cover in the course of any offensive cyber action. It was like threading through a bombardment campaign while being behind enemy lines.

"Signing our tools —" Lieutenant Arun immediately suggested. "Hmm — that would be too APT."

"We will get there, Gentlemen." Richard did not want to get to it until deeper defensive evasion classes commenced. He wanted the team to possess the knowledge to exploit that cyber power, as envisioned by the Colonel. That was because several elite adversaries were already signing their tool-work with the use of stolen keys for DET.

And the KDF was not going to be left behind.

CHAPTER FOUR

Offensive capability will always be vigorously pursued and actively implemented, for the conflicts to come. During war, cyber can be used as a shaping option, but sometimes, in cyberspace, shaping operations can also be a decisive move during actions-on.

The Captain and his Lieutenants were seated at the front. They were smiling at each other as they agreed on the impressive and ongoing cyber ops training. If one ignores the capability they were about to raise within the new unit, one would ignore the adversary intent coming in from the horizon. Information is the only domain, that ‘Troops In Contact’ is a constant from the adversary. The Captain knew at some point he would be the Major or Colonel in charge of Moran Cyber, and he would be managing OCO at fleet scale.

Richard walked to the whiteboard. He explained more about the hooking into specific APIs by the EDR’s DLL during, fore and aft monitoring. And the class seemed to enjoy and experiment further until when the Senior Sergeant raised his hand again. His voice had boomed as he asked for a small rundown on Injection Techniques even though they had already done the class a few days before their break.

Richard had no other choice but to comply. It was his job to explain until his teeth fell off. “We have self-injection and remote process injections as the main ones. We will discuss others later.” He expounded on both: How self-injection is solely on the PE with examples of when it unpacks itself. Then the remote process, especially on how the EDR would inject itself just after going into a running remote process.

He extended to write ‘LoadLibrary' on the whiteboard.

```
GetProcAddress(LoadLibrary("KERNEL32.dll"),OnTest)
```

Richard made a show of writing the statement from memory, on the board, in order to drive the point home. He had explained resolving. This was not new.

He turned, expecting a hand up. “By now I believe that everyone is aware and has practiced with LoadLibrary API, and has tested methodologies with APIs like CreateProcess, NtUnmapViewOfSection, VirtualAllocEx —” Richard exited the PPTs’ fullscreen and opened a TextEditor on his MacBook. He typed down the list from the beginning again. He exploded the fonts:

CreateProcess()
NtUnmapViewOfSection()
VirtualAllocEx()
VirtualProtectEx()
ResumeThread()
ReadProcessMemory()
GetThreadContext()
SetThreadContext()

Then he looked up. They were typing too. He said. “And others that I might have forgotten. Anyway, all this, is on MSDN. How copy?”

“Copy that.” Lieutenant Munga, also known as the class-time-keeper pointed to his watch.

Richard nodded at him for a second. Seemed like no one had noted the ambiguous NTAPI function, NtUnmapViewOfSection.

They had all moved on.

“Alrighty.” Richard tried not to snort. He had explained earlier how Kernel32.dll forwards its functions to KernelBase.dll and how that is important, during hooking and patching operations. He added. “So, if you alter a function on this DLL, the Kernel32, that same function can be used properly ‘cause it will exist in KernelBase.dll.”

The students had gone through the beginner classes during the earlier line up that almost had a hundred students deployed. They had already been trained in processors' architecture and where those DLLs reside for both systems.

Richard sighed and opened the Safari browser on his MacBook. He typed Google and searched, ‘MSDN GetThreadContext.’

“We search for one API as an example, just like we did before. Check.” Richard clarified on the function as he loaded the MSDN page for GetThreadContext API. “It will retrieve the context of the specified thread. The local pointer contest as you can see takes from a pointer context structure with the first argument being a handle to the thread where we retrieve the context. How copy?”

```
BOOL GetThreadContext(
  [in]      HANDLE    hThread,
  [in, out] LPCONTEXT lpContext
);
```

The students nodded like they were in a traditional society group.

They seemed to have been overwhelmed. Theory sometimes would do that to engineers. Technically solving problems was otherwise church.

“Okay, I know it's time for a break.” Richard acknowledged to all. “So think about these APIs, think about DLL Injection when on the break. Think about those functionalities we talked about when allocating memory. Then how LoadLibrary API is called. The arguments that are passed by LoadLibrary such that the DLL is loaded. How copy?”

A small murmur rounded up the room.

“Alrighty, let's come back at 1130hrs, and we get it going.”

“Alright, thank you Mr. Mbatha.” The Captain stood up. “That’s almost two hours of tea break. Let's keep time and be back here for the next session.”

All of the students stood up and most of them yawned. A few acknowledged the Captain's statement, saying, “Yes, sir!”

They were all in uniform that showed rank as it was a requirement in the Garrison. It probably was. Orders were orders. Even during computer classes or a garage sale.

Captain Eric Mwangangi walked over to where Richard was, “Hey Richie.” He said and pulled a chair next to him. “Got a minute?”

“Yes sir.“ Richard answered like he was still in the army, but he had left a while ago due to bureaucracy. He wanted to subsist into cyber back then. After stuxnet, the field seemed more interesting. But they kept sending him to the gate guarding duty and sometimes the armory.

The Captain pulled the chair back. He collapsed into it.

“Niambie?“ He asked him in Swahili, wondering what was on the Captain’s mind.

“We have a small issue. That we might need your help on.” The Captain said. “If you don’t mind.”

“Okay.” Richard paused on the message he was typing. He had unhooked the HDMI cable from the big screen to reply to an urgent email from Emmanuel, the CEO Secure Ark Cyber.

Emmanuel was also a former Colonel in the Directorate of Military Intelligence. He had opened Analytic Platinum Investigations when he was still in the DMI. Richard was one of his first employees and a former military Senior Sergeant. The company was then taken over as a cover company by the intelligence services to support Cyber innovation when Moula Bukstein joined.

Richard asked the Captain. “What’s going on sir?”

The Captain responded and in thought. “We have a developing issue that might require hands on deck if it worsens.”

“Check.” Richard swiveled round his chair to face him.

“We have data that has been pulled out of a certain location by one of our ground operators in Ethiopia. I have not been fully read in. But Colonel Cyber wants me and my team and your team on it. Since it's approaching December, we can work it and then continue classes on January.”

Richard’s mouth was open like he wanted to say something, although the Captain was still talking.

“I know it's unique to ask you this, but what do you think?” The Captain asked after realizing Richard was considering a remark. He waited for almost a minute.

Richard finally asked, “Have you talked to my boss? Retired Colonel Emmanuel? And also my immediate boss, Moula?”

The Captain shook his head. “You think it's necessary?”

“I think—” Richard sighed. “I think, it’s protocol.”

“One issue Richie. Moula can’t be involved, so we can’t have anyone else connected to Israelis and to the Ethiopians. It has to be closed access, need to know.” The Captain explained. “This issue is dire to National Security and as you can see, the elections are next year and such a threat needs to be dealt with before 2022.”

Richard swiveled on his chair again and rested his arms on his knees. “I understand what you are saying sir. Although, I think we need a discussion with Colonel Cyber on this subject. We have to get a background of the problem statement and also we have to include Retired Colonel Emmanuel in the discussion. There has to be an agreement. Even if we know who really owns Ark Cyber.”

Captain Eric Mwangangi agreed, “I think that can work and the team can learn on the operation too.” He paused as the last student left the hall and out to the stairs that connected to the library. He glanced at the big TV and said, “We can have a call on

Signal with Colonel Cyber and see what we can do next, then you brief Col Emmanuel after class."

"Roger that sir. I am available." Richard supplied as the Captain got off his chair. He knew this might end up being an OJT—On-the-Job Training kind of operation. It was the second time throughout his teaching career that a class went from ranges to OJT.

"See you after tea break Mwalimu Richard Mbatha." He told Richard feigning a salute. "Thank you for this; we are learning a lot. "

"Roger that sir. I appreciate."

CHAPTER FIVE

API Hooking class had to be postponed to 1400 hrs. This was due to the fact that two more students, who were Army Corporals, had requested a thorough class on DLL Injection.

Senior Sergeant Duncan supported the initiative and the Captain with his Lieutenants didn't have grounds to oppose. It seemed like they also wanted to be there for it and get more practice, even though PE format classes scared them more than gunfire did.

Richard decided to take time on it. He utilized his fifteen minutes of the lunchtime break inventing his own questions and simulations for that class session. The class discussed Remote Process Injection in far length than the earlier classes.

They practiced with MessageBox on a DLL.

They performed PE injections and started process hollowing before the lunch break. That went on for almost an hour.

Lieutenant Munga pointed at the clock. Richard indicated it was a negative. They got stuck on how to suspend the target process. Then they played with Early Bird APC Injection. Eventually Richard announced that they were ready for API Hooking class by 1400 hrs, just as the clock neared a few minutes to 2 PM. They had rented more time than allowed, on the earlier topics. And it was carrying on well.

Everyone was sweating by the time they went for the next break; lunch was a quick touch.

Richard switched on his phone as he dragged his legs behind the Captain, back into the classes' hall. They quietly passed through the library. Faded stickers had well designed camp's standing orders. A large sign at the door warned everyone that masks were mandated. No one in class had obeyed any of those orders.

"They should stock up on more modern books." Captain Mwangangi said looking at him. "At least something from Mark Owen."

"Hmm." Notifications slid down the screen. Rachael had tried to reach him.

"Richie?"

Richard was still on his phone. “Sorry?”

“I said the books. They need to bring in new ones especially on the kind of stuff we are learning in class.” He said pointing at the library. “Like Mark Owen books perhaps.”

“Definitely sir.” Richard agreed but he wasn’t following. “Do you mind if I find you in class?”

“Richie.” The Captain stopped in front of him and quietly said. “Remember we have that call with Colonel Cyber after today’s session.“

“Roger that sir. We will end the class early.” Richard said. “I can see my wife was trying to reach me. Give me two minutes, I will be right there.”

The Captain gave him a nod and turned for the stairs.

Richard thumbed through his phone:

Hey hon.
Class was busy today. We just had a brek.

She replied almost immediately:

Hi Boo. So sorry to disturb u. U k?
Winnie was sick, I needed help, I was stuck in the courtroom.

Richard studied the WhatsApp message and then quickly replied to his wife:

Rachael! What happened?

Rachael replied. She always typed fast.

Funny she was just gassing up.
And her stomach was swollen.
My brother came through. He picked her up, they r both at home.

Richard twisted his head and looked up to the hall where the class was. He knew it was those sweet potatoes his kid ate yesterday. He gawked at the thought. The Sunday afternoon brunch, after his mom visited. They had to wait for her because she had travelled late. He replied,

Those Grandma sweet-potatoes!!!

Rachael replied with a WhatsApp sticker of the laughing Kenyan President. She had totally copied several of them from Richard. Hunting stickies was now becoming a thing.

Richard sent a smiley back and then replied,

I gotso 2 go. I will be offline again.
I see u guys on Thursday?

His WhatsApp dinged back.

Will miss you.
Stay safe Daddy, we speak in the evening.

Richard switched off his phone. He held his breath. He wished he was home. He shoved his phone back into his pocket. He tried to pull himself back into the moment, and turned to the stairs leading to the class hall. The students were walking around sharing their class experience, and a few of them practicing on Process Hallowing because it was the favorable part of the class. Still, the technique would rarely be utilized in the battle-space. But the students were always urged on learning how to execute it in a lab settings.

CONOPs do change and the operator who innovates and evolves prevails.

"All right ladies." Richard turned on the big screens and logged into his laptop. "Three mikes and we continue."

With his announcement, the Lieutenants and the other students were back at their desks and logging into the laptops. After a three-minute wait, Richard nodded to the timekeeper, indicating that he was ready to proceed.

Lieutenant Munga glanced at his watch and then the hall's clock. "Check."

"So. The DLLs." Richard opened Visual Studio and told everyone. "Get VS up and set it for a DLL project."

"Sir." One of the Sergeants had a concern from the back. "A moment sir, my Windows machine is misbehaving."

It was a new laptop that had just been reinstalled with Microsoft Windows 10. The occurrence was more frequent than you can imagine whenever several IDEs were active on any operating system.

"Sir." The Sergeant called. "Might need to reboot the OS."

"Alright Silvanus." Richard hollered back. "Two more mikes, reboot. Everyone else, make sure VS is up."

After Sergeant Silvanus' laptop came up, he yelled from the back again. "Good to go sir."

"Copy that. Good to go." Richard returned the call out. "Alrighty, get VS up, create a new project and let's call it API Hooking. Make the project a DLL. Just like the way we had created one earlier, when we were building the other DLLs. That should be on General properties. On the General tab under C/C++ go to Warning-level and change that to — *Turn Off All Warnings*."

"Sir?" Senior Sergeant couldn't help himself. "Please slow down. Allow us to get to it, sir. It's a little complicated. One mike."

Richard guessed the team was not used to it yet. They had done this a couple of times to execute it blindfolded with a gun cocking nearby, but still, he gave them that minute.

"Sir." Senior Sergeant nodded. "Please proceed."

The time-keeper looked at his watch. The Senior Sergeant seemed to understand the signal.

"Copy that Senior Sergeant." Richard took the silent indication between them for concurrence. "Go ahead and remove the SDL; we don't need that either. So set No. Get to code generation. We will work with Multi-Threaded. If yours isn't on that, set it and then remove the security check. How copy?"

Sergeant Oyanga who rarely talked said. "Copy that."

Richard watched him cover a large yawn with his hand. There was a small mumble from the back of the class. He had talked by accident.

"Alright, alright, alright, all right— Alrighty." Richard clucked. "Glad to see you are still with us Sergeant Oyanga."

The entire class erupted into a chorus of loud ovation, taunting him.

"Alrighty alrighty." Richard joined in the applause. He could see Sergeant Oyanga was the type of man who hated attention. He was also an observer. He would have done well in field operations and interrogations. "Let's get back to it gentlemen."

"Thank you sir." The silent Sergeant gave a curt salute. "I am good to go. We can proceed. Sir."

"Okay Sarge." Richard continued. "Get to the Linker, just below. Please look up on the large screen, ladies."

Everyone glanced up to confirm the tab and then went back to their laptops' screens.

"Yes, you got it." Richard appreciated their clicks. He moused up. "Set that to subsystem Windows. Yes, we now have it. Oh, we forgot the Multi Byte. Go back to general and set that up. Remember we played with PE Headers before and parsing them accordingly. We will need to do that on this project too. From the Dosheader, all the way down to stuff like thunk data. And yes, for a dll like ntdll.dll —”

“I still don’t understand why we need this DLL Mwalimu Mbatha.” The Captain asked. He was tense. His comment obviously had to do with PE format. It was a nightmare for most. “Sir, do we really need to build a new project?”

“We are getting on that Cap.” Richard got up and paced near the screen. “Like I introduced it earlier on Friday, API Hooking is kind of a way to change how an application is executed in memory. Best examples are game cheats. The crackers usually pull API Hooking techniques to make a player return healthy throughout the game, by the use of debuggers. Actually, let’s use a debugger for this example, to make it clear. Hopefully from this, we can understand the reasons why when we push our DLL.”

“Thank you.” The Captain nodded. “We appreciate that.”

Most cyber ops classes required a degree of simplicity to guide students toward a clear understanding of the technical capabilities needed in the engineering of well-developed CNO toolkits.

“For now, minimize VS gentlemen. We will code that later after we see what the debugger will do on a process. We will definitely work with the .text section.” Richard dropped back into his chair heavily. “Today we will be closing earlier because I have a meeting online with Colonel Cyber, or rather Colonel Mutama.”

The Captain had emphasized the significance of the meeting, despite Colonel Cyber's aversion to online meetups, even during Covid.

“So let’s try to finish up on as much as we can. Let’s say by four pm I hope.” Richard leaned back in his chair. He arched his back, and stretched his arms. “The rest we can continue tomorrow.”

“Yes sir.” The Captain agreed.

Richard asked, “Any other questions so far?”

Everyone was busy on the computers.

“So.” Richard continued, “Make sure you have xdbg installed, both x64 and x86. Also confirm you have Process Hacker installed. Once ready, lemme know we fire the grill for this one. Time-keeper you got this?”

Lieutenant Munga answered. “Check.”

“Copy, five mikes.” Richard noted back. “Also if you didn't have IDA Freeware on your Windows machine as instructed earlier, make sure you have it up. That’s for those who haven't installed it. Okay? Alrighty gentlemen. Go. Five mikes. Make sure you have it installed.”

Once everyone had IDA up and Xdbg, Richard asked them to run x64dbg from their Windows computers. “Lets understand it from a RedTeamer or CNO developer point of view. We will use a Microsoft Windows process like cmd.exe for this. You can try calc.exe or even notepad.exe, copy?”

Everyone was running through the keyboard and checking their screens to make sure they were on the same status with the main trainer’s television screen.

Richard was making sure every step was picked up by the students at the back. They are usually the ones who were easily lost. At some point he wanted them to move to the front seats even though the senior officers were there, and had taken up positions.

“Gentlemen, load cmd.exe. My process check — for this command line is on that PID. To get it, you can use task manager or basically do a tasklist with a findstr of cmd.exe on the same command line.”

The students glanced up at the screen, and Richard wrote down the commands on his active command prompt for its process.

```
tasklist | findstr cmd.exe
```

They understood Microsoft Windows command line because it was the most basic ICT resource any one could have.

“Remember the PID number. It's going to be important because we wanna attach it to the xdbg. Though I think you can still attach as a process. This process is an x64 process ‘cause all our machines are running x64 Windows OS. If you wanna confirm, check the processes’ image, with the Process Hacker tool.” Richard opened Process Hacker with administrative privileges. “Make sure you ran it, all privileged.”

The UAC prompt shot up and he waited for a minute to make sure all students are there. Then he allowed the prompt to execute and clicked the tab Processes, and casually made sure all the processes were arranged alphabetically.

“Alrighty, once on properties.” Richard right clicked on the cmd.exe process and rolled through until Properties. “Just right there on the right part of the window and we have, Image Type. And that’s 64 bit, just right there. So let's debug with x64dbg.”

Some of the students were back on their notebooks, drawing or scribbling some notes.

Richard paused and waited. He wanted to ask each and everyone, if they had followed the instructions so far.

Instead he urged. “Any questions so far?”

“Sir.” Sergeant Silvanus at the back went for it. “You had said that 64 bit Windows binaries are at the System32 folder and thirty-two bits are on the SysWoW64. Is there a reason sixty-four bit should be the one running by default?”

“By def, yes. But you can still run cmd.exe from thirty-two bits’ folder. By this example, if you do, then the memory addressing and some calls during debugging would look different for you on your template, especially as you step on it with the class on the debugger.”

“Okay.” Sergeant Silvanus was nodding before he finished. “32 bits versus 64 bits.”

Richard volunteered some quick code. “Let’s say we are performing low level search to identify base address of the image in memory."

```
__asm

{
        mov eax, virtual_address
        and eax, 0xFFFF0000
        IterateImage:
        cmp WORD PTR[eax], 0x5A4D
                je EndIteration
                sub eax, 0x00010000
                jmp IterateImage
                EndIteration :
        mov [image_base], eax

}
return image_base;
```

Writing ASM, especially in front of the class, took time. Everyone was up like they were sizing each other.

Richard swallowed down the intensity. “The image_base is a pointer that we initialize as zero or NULL.”

Sergeant Silvanus insisted. “The MZ.”

Richard had to redirect this before he put more on PE’s structure. “The memory on hexadecimal value shows we are dealing with x86 memory of this iteration. And so, if we had x64, how would it look like?”

“Longer?” Captain Mwangangi chided in.

“Exactly” Richard re-wrote the code:

```
{
        mov rax, virtual_address
        and rax, 0xFFFFFFFFFFFF0000
        IterateImage:
```

```
        cmp WORD PTR[rax], 0x5A4D
                je EndIteration
                sub rax, 0x00010000
                jmp IterateImage
                EndIteration:
        mov image_base, rax

}

return image_base;
```

“You see the difference?” Richard knew from experience that working with __ *asm* on 64 bit wouldn’t be applicable for this example. “I hope this makes it clear. How copy?”

“Copy that sir.” Sergeant Silvanus hindered his frustration like other students did whenever they labored with debuggers and assembly.

“I know it's a lot to catch on, but you will all get there. Let’s continue.” Richard loaded his x64dbg toolkit back up. “As you can see, aah— my debugger is on the taskbar. What I wanna do is click File and then Attach button, and that will attach my process.”

Most of them were familiar with xdbg especially from earlier classes. They had even debugged live code with other trainers like Moula Bukstein. They didn’t mind being trained on that again. The problem arose when working with NTAPI functions later on.

Richard moved his mouse up to the left of the screen, opened the File tab and punched attach. He scrolled down to where cmd was hanging out. He needed them to make the connection.

The students followed.

Richard directed them. “Once there, just click cmd and the process will load on the debugger. Just like that.”

The whole class did the same as the trainer illustrated.

“Once we have this process hooked, please click Memory Map, it should be the fifth button from the left.” Richard said and run the tabs slowly for them. “Once there, scroll to the .text section of that process. Remember that processes’ name.”

There was a hand up.

It was Sergeant Silvanus again. “Sir?”

The Captain looked back but Richard had already signaled him to continue and ask.

The Sergeant went ahead. “These are the same sections we were seeing during the PE classes?”

“Yes, exactly.” Richard gave a short answer sparing him another long lecture. “You will need this when pursing the target process during API Hooking. I hope you all remember how we parsed them earlier?”

There was a small murmur again at the back. The hate for PE format was visible in the air, like a fog.

“Sir?” Sergeant Silvanus extended his question because he now totally needed to press further. “And on the debugger they are actually telling us what each section means, but the C-F-F Explorer didn't show us those names?”

“By their names. Yes, Sergeant.” Richard answered and then decided to explain, “That’s why I always frequently say, open these Microsoft Windows PEs, each time you get a chance. Learn through them. Experiment. Again and again. And you will learn so much than the normal cyber people who just troll through blogs and tweets all day. Go check on them, from MSDN and work through undocumented APIs. Load ntdll.dll on IDA and look at its exports. The ETW exports, the NT exports. It’s importanter.”

“Copy that sir. Thank you.” Sergeant Silvanus nodded approvingly. A brief acknowledgment etched on his face, before seamlessly returning to the rhythmic barks of his keyboard. He was probably firing IDA and then checking the imports and the exports and probably had just realized, ntdll.dll doesn’t have as many imports as exports.

The Captain looked back at the Sergeant and gave him an inquisitive smile. He was the most active serviceman even if he was sitting at the back. It's like if he had been asked earlier, he would have sat next to Richard and ask more questions slowly, and quietly because he wanted to know everything.

Richard went on. “As you can see. At the screen gentlemen, at the screen —” He waited for everyone to look up. “The .text section is where the Executable Code is. The .rdata is where the Read-Only initialized data is. And so on and on and on. Everyone copy?”

Sergeant Silvanus was the first to nod. He was back on his keyboard experimenting again.

Only the silent Sergeant seemed sleepy.

“Hey!” Richard called out his name. “How are we doing Sergeant Oyanga?”

He didn’t even look up. He was set and back on his keyboard.

“Alrighty. Let's continue.” Richard feigned agreement. Never press a silent man, for they already know their route out.

CHAPTER SIX

Richard right clicked the .text section and arrowed the mouse pointer on the: Follow in Disassembler. He edged at a memory address that showed several CCs also known as int3 instructions. “You can see those int3 instructions. On my end its on 07FF634161056, check what you have. They should be several.”

The students continued on their screens as his intriguing patience of the trainer-in-him taunted him to wait. He stood up, paced behind the desk, and then moved to the big screen. He stuck his hands into his jeans and waited.

Then waited some more.

“Sir.” The timekeeper said. “All good. Continue.”

“Okay,” Richard sat back down. “So check on Process Hacker for the cmd.exe process. Go to properties. Click the tab memory and scroll to the address where we had the int3s.”

All the students were now cracking on their keyboards.

Richard had to pause again to make sure they find the base addresses. He wanted to stand and pace again. He wondered where the impatience was coming from. It rarely overwhelmed him. He had guided them through Visual Studio’s disassembler during a process PID hunt with Windows API and NT API a few weeks ago. The first time he did it independently, he felt completely badass—until he repeated the same process on a DLL project with Visual Studio while the PE was running remotely for a memory walk.

“Oka — aay.” He decided to offer. “It should be where the process is, the cmd.exe process line for the image.”

Everyone was buried in their keyboards.

Richard moved his mouse and cornered it over to his ‘image commit’.

Sergeant Silvanus whistled. He was the first to catch the section and get the instructions.

“That’s right.” Richard hovered the mouse over the screen, ensuring everyone could view it. “There. Let’s go gentlemen. Let’s dig in.”

All the students momentarily shifted their gaze from their laptops to the big screen, then back to their laptops, and once again to the screen.

Richard checked his phone which was still off. He turned back to the class. “It should be on the .text segment again and mine shows that it's mapped at 0x7FF634161000. That’s where mine begins. Check?”

“Copy that.” The Captain hustled on his keyboard. “I have it too. Check.”

“Anyone lost?” Richard asked.

Most of the men appeared to grasp the concept, a collective understanding settling in the room.

Richard tried to find the silent Sergeant. Routinely, the man was dodging him.

Sergeant Oyanga glanced at his partner’s computer.

Of course Richard decided to give out two more minutes. “Two mikes. Find the address.”

Sergeant Oyanga hustled. Then he at last looked up at Richard and smiled.

“Good stuff. Let's continue.” Richard gave him a subtle nod, acknowledging the man's accomplishment. “Double click and you should see those int3s.”

Oyanga did it and another box shot up.

Richard watched him work the keyboard.

Oyanga almost spoke but he was distracted by the other servicemen as they looked for their first int. They were hunched down on their keyboards.

“Slow down.” Senior Sergeant Duncan yelled at last. His voice covered the whole floor. He was obviously frustrated.

Xdbg would do that to you.

There was a small laughter from someone on the senior officers’ side. It’s like they were expecting his scream because things-assembly were always tight for the Sergeant.

When Richard studied Assembly on his own, it was a headache. Either he had to go look for rent or understand the parameters for x86. Then later on, came the x64. Then he had to interact with MASM for Win32 ASM. Nothing was the same after that.

“Cool down gentlemen.” Sergeant Duncan laughed back, with that snarky smile that felt like he was mocking everyone. “We will get it.”

“I’m sorry sir.” Oyanga tapped his keys. “A bit lost but I’m finding you. Stand by sir.”

“Standing by.” Richard replied and leaned onto his trainer’s chair. He was given the biggest and the most comfortable seat, pulled deep from the nearby offices. He stretched his legs up, in wait. He said. “You got this Senior.”

After a few minutes, Senior Sergeant confirmed. “We have it.” He was not the only one near his desk that had got lost. The other Sergeants, near him looked amazed and glad they found the memory’s base address.

“Good stuff.” Richard got his legs back down under the desk. “As you can see after the CC, CC, CC — all the way to the finish line, my next instructions are 48 8b 49 78. I’m gonna set a break point on that — for the debugger. How copy?”

Several officers replied, “Copy!”

“Good copy.” Richard gave a pleased sigh without deciphering their tone. Assembly was not a cup of tea. “Charlie Mike.”

Sergeant Oyanga muttered something.

For once, Richard didn't want to ask. He moved his mouse and selected the instructions and then went back to the debugger to confirm them. He was back to his in-training self. “We will set a breakpoint just after those instructions and so with that, we will use the 48: 8B49 78. Go.”

The students hustled.

Richard didn’t wait.

The Captain glanced at the back again. He gave a resigned sigh when he looked back to his screen.

Richard said. “Let’s set a breakpoint here.”

Everyone did. Or tried to do.

Richard right clicked on the memory region. He clicked a Breakpoint. He followed to the next column and moused a toggle.

The Captain flashed a self-satisfied smile. Most of the students by now had a good experience with the debuggers even though assembly was a headache.

Richard said. “Two mikes to get there.”

That was for those who were still struggling with the routines.

Several had the breakpoint up within the first minute. A few had it later and they started to alleviate from the ASM turmoil.

“I hope *ugali* wasn’t too much.” Richard chuckled. “All that starch slows you down.”

The class laughed.

“Alrighty alrighty. Now if you go to the Process Hacker, you will note the point where we had a byte at those locations we were looking at have been changed. Confirm. It’s a little change, but you get the idea.”

“Not yet.” Lieutenant Arun mumbled.

Richard noted there was an issue and outlined the 0000060 line and said. “See on my end, now I have CC 8B 49. Check?”

“Oh — Ah!” exclaimed Lieutenant Arun. He was the first to capture the change. “I have it. Thank you sir.”

Richard nodded and continued. “So, as you can see, we can change what we are seeing in the memory but it's hidden on the debugger which is different on the running process in memory. So in this memory the instruction 48 is gone. Pwah! Just like that. So for us to understand all this we will start with the Import Address Table, get IAT API Hooking to the works. It can be real good during ops and for CONOPs development.”

Of course the students had to agree as they waited for fresh examples and an expounded methodology. C/C++ was next up in queue. They all had to endure the afternoon.

“Now, this is how API Hooking works. But we are going to use it for offensive means because we want to penetrate the enemy. We wanna collect. We wanna impose costs.” Richard coached. “The methods out there are different. Adversaries have come up with several techniques. Like I had said before, now you will all see why you need to understand more of the PE format. Just like in the Process injection and the PE infection class, and the PE packing classes earlier. Oh, and not forgetting, those classes on the PE compressions which were a disaster — though very *importanter.* The PE format will be very essential hence forth.”

Everyone hated PE format classes from the last month to now. The PE compressions to sections was chaos since day one. They also disliked it when Imports and Exports were introduced for the first time, especially at the beginning of the main classes. It was a nightmare, and still they hadn’t collectively appreciated it.

Maybe it was because of the pointers.

Undeniably the filepointer.

The Relative Virtual Address, RVA.

It was clear the students got tensed every time Richard mentioned those earlier lectures.

Moula had dropped them into a rabbit hole and she left them there. The dropper class. The XLL class. The XLLs zipping and zapping trick on AppData. The C# Command and Control listener class. VTSO for initial access operation’s class.

Richard realized they were somehow terrified and a little out of sync. He knew how practicing and the in depth late night research had helped him when he started.

Facing off with ASM and then understanding PE structures was like mounting a new war that most didn't understand.

Richard had to shoulder part of their burden. “We can repeat the PE format slowly tomorrow morning, if that’s okay with Cap.”

There were smiles at the back. It infectiously came to the front row. The Captain agreed to the novel initiative. This was not new for him; he had some experience with PE Headers from attempting exploit development classes in Tel Aviv.

His fellow officers too, seemed like they agreed.

“Alrighty. That’s a date, gentlemen.” To his credit, Richard hustled them as he lifted his hands up into a wave. “Alrighty PE Format, breakfast date.”

There were some chuckles that died quickly as they tapped their keyboards.

“We have around 30 mikes to get the DLL ready. We won’t do much on it today, but let's prep the leg work. Just like we did, with the example DLLs before.” Richard turned his attention to the laptop. “We played with DllMain, the dwReason. All of the required DLL scenarios. So, I believe this should be a piece of cake. Let’s go gentlemen. Get to VS.” Richard brought his Visual Studio up. “Add the cpp file, make sure you are not on release mode. So the properties we changed should correspond with the environment. We will do this on x86 for now, so remember Debug x86, as shown on screen. Let’s go gentlemen.”

The whole class re-did the configurations afresh for the API Hooking properties’ project. Richard walked around the hall making sure everyone was on point.

The officers were the first to complete.

Sergeant Oyanga kept checking on his partner’s work.

Richard allowed it, as long he did the code and made sure he was solid. Military operations even during CNO, had to be done in team work as always. This was in order to save lives and ensure the operations were effortless, smoother and faster. Some of the students in this class would end up working in the field running close-net operations behind enemy lines. They would join the team that ran such operations codenamed CMOF, in full the Cyber Mission Operations Force. They were usually strapped to the Special Warfare military groups in the field and the National Intelligence Service paramilitary sections.

The students had to get better.

They were meant to be the absolute best CNOers in the different units, collecting Signals Intelligence during warfare and peacetime.

They had to do the work.

Richard doubled a few more paces across the hall and then threw himself back to his chair.

“I hope we are set.” He asked. “Good to go?”

Sergeant Silvanus joked. “Afande!”

Richard watched as he compiled his DLL. He was always the first serviceman to have his project online. Sometimes the Captain would be the first to complete the task, but rarely. He had some background in C/C++ and C#. Though, Windows API and NT API had slowed him down in class most of the time. The Israelis in his exploit development class had obviously not gone the extra mile.

Richard had to bend the truth. “It will get easier.”

Sometimes it was more motivation too, because everyone hurried to get their code done.

The serviceman would take in the first gear like always. It was a learning curve for everyone.

Richard went back to his keyboard. His training laptop had locked. He quickly typed out his long ass password. Visual Studio popped out and the screen reflected back onto the students. Richard went ahead and said. “As usual we need to import windows dot h, by including it.”

```
include <Windows.h>
```

He looked up and most of the students who hadn’t done the code were now doing it with him. Sergeant Silvanus was not typing; he was just confirming whether he did the right thing. Richard smiled back at him, because he was becoming his best student. He didn’t want the other students to buy that, so his grin slowly turned into a smirk.

No teacher wanted to show favoritism.

Richard repeated. “Include Windows dot h.”

The officers who were near his desk were impatiently waiting for the next line. They looked up at Richard like the grill that does not start on 25th of December.

Richard unashamedly decided to continue. He said. “Call the bool winapi because we need to work with dllmain. The parameters as usual are Histance, a Dword and a local pointer void. Then we need a switch it up, so that we check if the dll has been injected, rather attached.”

Senior Sergeant Duncan coughed like he was complaining at the trainer even though that cough was not wet and real.

And then Richard looked up to check on him and the Sergeant eyes wandered over to Sergeant Silvanus. He was checking if he had changed anything so that he can do too. Then Richard’s focus was on Oyanga. He had to make sure he was still with the class. He was always the silent one.

Richard called it. His voice was hard as steel and loud, almost like a joke. “Alright, go return. True! As you know, if the function fails, then it's false. *False*.”

```
BOOL WINAPI DllMain(HINSTANCE hinst, DWORD dwReason, LPVOID reserved)
{
        switch (dwReason)
        {
        case DLL_PROCESS_ATTACH:
                break;
        case DLL_THREAD_ATTACH:
                break;
        case DLL_THREAD_DETACH:
                break;
        case DLL_PROCESS_DETACH:
                break;
        }

        return TRUE;
}
```

All the students went on, and tried to compile.

Some were still having errors.

Silvanus was the first to discreetly guide them in checking that their project properties were in order, particularly for a DLL project.

“Yes, like Sergeant Silvanus said, check your properties.” Richard agreed. He was wondering why they would forget that. “Now, on the DLL process attach, that’s where we will set our Import Address Table hook. Hope you all remember the IAT?”

Keyboards punched, barked and rocked the room.

Richard added. “I am going to add a call so that the DLL can be loaded with Regsvr32 instead of rundll32. The DLL will just display the computer name via MessageBox for this example.”

```
extern "C" __declspec (dllexport) int DllRegisterServer() //Regsvr32.exe as proxy (DET)
{
        wchar_t endPointName[MAX_COMPUTERNAME_LENGTH + 1];
        DWORD size = sizeof(endPointName);
        if (GetComputerNameW(endPointName, &size))
        {
                MessageBoxW(NULL, endPointName, L"Target Computer Name: ",
MB_OK | MB_ICONEXCLAMATION);
                return TRUE;
        }
}
```

Richard waited. “Note the DllRegisterServer export.”

There was a murmur. Everyone was paying close attention now.

“General, then configuration type. Dynamic Library.” Sergeant Silvanus commented, because he was so smart at the moment. “Thats for DLLs.”

“We discussed the IAT several times gentlemen.” Richard gave the Sergeant a crooked smile and decided to ask all the other students again. “Especially when we were looking at different PEs on IDA. I hope you all remember?”

Rather than scanning everyone, his eyes landed on the Captain's.

No one answered.

Richard clenched his jaw. He knew there was a problem. He wasn’t sure whether to repeat the IAT class or go ahead on showing them how to hook on it during offensive operations. He smiled but all he wanted to do was to throw something out of the hall. He was a better trainer, all right. He knew how to calm down faster than Moula Bukstein, his training partner.

If it was Moula in the class, she would have lost her shit by now.

Richard gave Sergeant Silvanus a sideways glance. “Sergeant, you remember? Or you marked it as EOD and got your ass out of dodge?”

Everyone spilled a deadly laughter. Richard knew how to lighten the room when there was immense tension.

“This requires some more research sir.” Sergeant Silvanus finally answered. He wanted to stand up but he continued mid laughter. “I remember the imports tab from IDA and the parts on image import descriptor.”

Richard waited for the laugher to die down. “You are on the right path Sarge. Please everyone, go back to the videos tonight.”

Everyone looked up.

“Remember the Original first thunk which points to the Import lookup table.” He demanded. “And the first thunk which points to the Import address table?”

All students nodded because they seemed to recall the class.

“Okay.” Richard assumed they had. “When the module is loaded into memory as a process, the PE loader has to parse this as it reads the Hint Name table so that it can get the name of those functions which are filled up on the Import Address Table.” He stood up and continued. “On the first classes about the loader, we discussed Windows Debugger and walked the PEB. Check that too. It's going to be important moving forward, when we start the CNO Tooling class.”

Lieutenant Munga signaled his watch at Richard. He was insistent on timekeeping.

"Copy that." Richard assented. He had to grant the students enough time to prep for tomorrow even if it affected the timetable.

“Class is dismissed until tomorrow afternoon. That will be enough time to do the research necessary, and the reading required.“

The Captain stood up too. “Thank you Mwalimu. Like we have been asked, let’s get those done by tomorrow, so that we can have the class up and flawless, when we are back.”

Richard remembered that he had to upload the current class videos to the portal. It was just some SFTP commands and then linking the MP4s with href video tagging. HTML5 had made working with jQuery pretty resourceful.

“Mwalimu Richard.” The Captain turned to Richard and asked. “What about the PE Breakfast class?”

“Let’s push it to tomorrow afternoon.” Richard laughed. “Something like a brunch bros-date.”

Everyone agreed.

Richard added. “Remember, during CNO, stealth is always your friend. In some infrastructures, a small detection and you aren’t ghosts anymore.”

The officers in front glanced at each other and one shot a slow smile at Richard who nodded back at them both.

Lieutenant Arun mouthed something about the call.

But Richard checked on what Sergeant Silvanus was up to. The Sarge seemed havoc busy. He was engrossed into troubleshooting an error. He glanced up and furrowed his brow at Richard, gradually creeping off an approving gaze.

The Captain said. “So enjoy the evening everyone. Mwalimu, we have been asked instead of a call, we head to the DIA’s office downstairs. They are waiting for us.”

“They are here?” Richard kept his expression guarded. “Who and who?”

“Colonel Mutama and Brigadier Thuo.”

Richard felt like he had been asked to the headmistress’s office.

CHAPTER SEVEN

Brigadier Thuo, the current commander Military Command Center Corps Military Intelligence was in the room. He was accompanied by Colonel Mutama; aka Col Cyber, aka Director of Military Intelligence Cyber branch. They were both seated on the biggest and darkest office sofa that had wooden arms to give it a sleek finish, just next to the windows of the DIA's chief’s office.

The Commandant (Chief of the DIA), was not at the Garrison at the time due to another objective, but the Brigadier had commandeered the office for the meeting that might take most of the evening.

As usual, the office seemed bare. The only artwork was the President’s framed face. There were no curtains that softened the office. It was like the DIA lived in the battlefield even after the promotion for well served tours in several conflict zones, around Africa.

Captain Mwangangi had been the first to enter. He had billowed a foot-stamp and then slapped a salute. “Sir!”

Richard Mbatha walked behind him at the time. He had paused and saluted too, though it was not required of him.

Incidentally, he was glad he wouldn't have to do that again as a civilian.

Both senior officials were dressed in their full military uniforms and the only distinctions to Captain’s was their gorget patches and ribbons.

“Welcome Mr Mbatha.” Brigadier Thuo offered Richard his hand. “How is Emmanuel?”

“He is okay, sir.” Richard shook his hand hard, noting that Brigadier Thuo seemed unaware of his military experience.

“And Anthony Mburu?”

Richard silently careened through a series of embarrassing answers about Anthony: Drunkard. Man whore. Raging asshole. He settled on, “He is okay. Still struggling to get back up.”

Colonel Cyber nodded them to sit. He had steepled his hands in silence.

“Is he still drinking?” The Brigadier had to ask. “Last time I saw him, he was high as a kite in the office to even recognize his former boss —eh!”

Colonel Cyber made a low growl because he was Anthony’s former boss. He had never liked him. They all never liked him. Or maybe it was pity.

The Captain listened on. He was also expecting to hear the answer. He, too, knew Anthony well and understood what he had endured.

Richard made it to his seat. It was not his job to take care or follow on with the drunkard. He still answered. “The loss of his family still hits him hard, sir. Everyday sir. It’s like an open wound that never heals.”

“Al Shabab.” Colonel Cyber admitted. “What makes it hard, is that he watched the damage they did to his two kids. May God bless their souls. Anyway, gentlemen. Thank you for coming in.”

So it was pity. Richard said. “Thank you, sir.”

“We have an issue, that we think —” Colonel Mutama stammered a little, evidently unsure if he had permission from his senior to disclose the entire issue to the team. “It’s a developing situation that Brigadier experienced first-hand and —”

Richard watched him turn to the Brigadier. He had that permission look on the face, that you give your boss.

He told the Brigadier. “Sir, I think this team we have here, led by Captain Mwangangi might be of service and will help in carrying out your orders, plus follow-ons on the cyber realm, and then probably on the meatspace too. If required, sir.”

“Sir.” The Captain asked. “Do we scrub the current mission?”

Richard took his time absorbing the development.

“We are still in class, and no-where near completion.” The Captain added. “Sir, do we skip the classes and go hands-on, operations?”

Brigadier was still silent waiting for the debate to end. He crossed his other leg over his knee.

“I believe, Captain. We could be having a security issue at DoD and MoD.” Colonel Cyber glanced up to make sure Captain Mwangangi caught the drift. “I think we can have some good cover for this, as a DMI op. Running it as if it was a class. A class I believe is still ongoing. This is until we find out where the security threat is.”

Richard could tell something unexpected or critical, had happened. He cleared his throat. “What security issue sir?”

“There is —” Colonel Cyber tried to answer. He turned to the Brigadier. A subtle hesitation suggested a restraint in delving into the specifics of the issue.

“We have a *mole*.” Brigadier Thuo interjected him. He wanted to make it clear. “It’s a counter intelligence issue. We have an entity which has taken down one of our men in the streets of Addis Ababa. Actually at the airport during a hand-off. This entity, who took him down seems to have resources that we have yet to account for. He is well equipped. It’s probably a Nation state-led activity. We don’t know who yet, and we can’t attribute or take it to the Presidency, unless we are sure who is our main target. You understand?”

“Okay. Sir.” Richard thought that it clearly had to do with cyber. He had to analyze the situation differently even though he had to listen first. He rubbed his temples trying to stave off a headache. Glasses were going to be a basic need pronto.

“Ethiopian Intelligence?” Captain Mwangangi straightened his shoulders. “Sir?”

Richard coughed. “M23!”

“Negative.” Captain had decided to amend him. “M23 is militia. It doesn’t have such capabilities yet.”

Instead of shooting them down, the Brigadier and the Colonel both laughed.

Captain Mwangangi looked down at the table. The room was silent again.

Richard remembered in an earlier class, he had mentioned modern militia might start using cyber to destroy critical infrastructure of their enemy states. M23 seemed like the kind that would conduct cyber ops against Kenyan infrastructure, considering that Kenyans had planned to support the DRC army and counter a civil war in the Democratic Republic of Congo.

“Okay” The Brigadier pulled some huge files from his bag and spread them on the coffee table in front of them. “The General and the President feel there is a threat inbound. And I feel it’s already here ready to explode on our faces. I will need to know if you can establish a sober assessment and take control of this issue via Cyber given the current escalation.”

Richard watched him stub through the pages of one of the largest folders.

Brigadier Thuo pulled one of the files in the middle and opened it. “Gentlemen. This is our Asset, Gebre Kebede. He is from Tigray. He works for a company we have been investigating since last year.”

Tigray was not in the news as much, but people around East Africa knew that there was some form of larger armed conflict. And if the asset was really Tigrayan, this would become a diplomatic shitstorm for the State House.

Brigadier Thuo turned to his Colonel as a handover. “Colonel.”

Richard wanted to pick one of the folders. A photo had slid out. It depicted a crime scene in a parking lot. He looked up to Col Cyber because the blood was too much even on photos.

“Yes sir.” The Colonel stuttered. It was his in-thing. He stood up, bent over to pick the first file, and rearranged the opened one. “Gebre works for Biham and Associates, an Israeli company which has offices in Addis Ababa. HQ is at Tel Aviv. It's a defense intelligence contracting firm. It started as a tech company but nowadays it does other things as well. It’s also a PMC known as Vanguard Protection Group and also a lobbyist group named, Strategic Defense Initiatives. Code name for Gebre Kebede is Chematstone. He has been working for us, collecting intelligence on what the company is up to and its intensions in East Africa. The operation is task forced between us and the service.”

Richard knew he meant National Intelligence Service. He felt his mouth drop in surprise. They rarely task-forced such secretive and sensitive ops.

Colonel Cyber said. “The enemy was ahead of us throughout the operation because they had recruited someone from our side.”

“Sir, is Chematstone active?” the Captain asked.

No one thought to ask about the insider.

“We are not sure yet.” The Colonel let out a deep breath. “At the moment we can’t reach him. He was doing a meet the day before yesterday, with LT Nyalita, inside Bole. LT flew in, it was supposed to be a brush and then shots were fired. It’s a mess over there. The Brigadier just flew back today from Addis.”

Brigadier Thuo slumped back into his chair. The desperation on his face was still fresh.

“We can look at the footage and try track the shooters, sir?” Richard interrupted, then realized it was unnecessary. If DMI had the footage, then it would be a different Course of Action. He answered his own statement. “The footage is gone —”

“Yes, the footage.” The Brigadier answered. “The footage is gone. I was shadowed through the airport, two women at Bole and the same two women at JKIA. Ha! They kept bumping into me and I think they wiped the hard-disk remotely. The disk is dead. They even sat with me at one of the cafes. Bastards.”

The tactic didn't scare Richard as much as the first time he had heard of remote meatspace disk wipes. The Russians had deployed such tactics with the use of discreet devices that emit a strong electromagnetic pulse when placed near the target's electronic equipment.

“You know.” Brigadier Thuo turned into that meaningful look as he sat up. “I think they were Russian Foreign Service. Unless I am wrong, then it could be all white noise to distract us from their main objective or whom we should target. We may need the JKIA CCTV footage pulled.”

“Sir?” Richard asked. “So it’s either Russians, or Ethiopians or the Israeli contractors?”

“So who is our target?” The Captain seemed to have been caught off-guard by his question.

The room was silent again.

The Brigadier ignored it.

Richard felt himself start to catastrophize.

“Here.” Brigadier Thuo pulled the disk out from his bag. “We have some backups at the Embassy, Addis Ababa. The files are too large to upload or send via email.”

Richard took note of the ICT lingo. He briefly pondered how the Brigadier became acquainted with it.

The Captain picked up the disk, as if to inspect it for physical damages.

“Yes sir.” Colonel said. “Upload would take years. The Internet in Ethiopia is still highly regulated by their government.”

“And the two women, sir.” Richard asked. “Where are they now?”

“They took the next flight to Heathrow. We have asked the UK government to help out; we haven't got an answer. You know how the Westerners are. But we still need the JKIA CCTV.” He turned to the colonel, nodding for him to proceed. “Colonel.”

“Sir. Four days ago, Chematstone informed us that the company had pulled some cargo from Syria and flown them to Addis Ababa. Signals Intelligence indicates they were not arms or bombs, It was something else, but the order was from Ethiopian MoD in a collaboration with Eritreans. We captured that intel on a stingray too — as our second source.” The Colonel stammered a little, then coughed to try get his words in place, “We asked Ekraal to help with Initial Access Operations into Biham and Associates. The first attack Ekraal and NC3 team developed was squashed. The tactic employed was a malicious document sent over via an email to Chematstone. It was a bad move and it could have burned him.”

Richard understood the repercussions of poorly planned cyber operations—assets could easily be blown. Spearphishing with documents was a risky move; typically, only noisy crimewave threat actors executed such audacious IAO.

“According to the plan, Chematstone was asked to open the email that had that document on Friday and Ekraal personnel said they had updated their code. He detonated the document as instructed, and it was immediately caught by their security software.”

Everyone knew Biham and Associates was one of the high-end Defense and Intelligence contracting firms that had offices in East Africa. No one understood why they selected Addis Ababa for their main African headquarters.

“Sir.” Richard had to ask. “Why are we using maldocs at this age?”

He meant malicious documents laced with a staging code. Possibly VBA/VBS or PowerShell.

“MalDoc use is a very, very bad TTP.” Richard was ready to preach. “And, it is so, so — so 2000s. Every PSP will catch it.”

“Exactly. Those were the lessons learnt. We came to understand that the hard way, after burning the stealth needed for the op.” The Colonel caught a cough on the back of his hand. He looked at Brigadier again, with that face meant to ask for permission. “If I may sir, I would like to specify what happened after that.”

“Roger.” The Brigadier offered him. “Continue Colonel.”

“Sir.” Colonel Cyber nodded in acquiescence. He turned to Richard. “Chematstone was asked to find a way to get all documents related to the shipment. He had to wait until nightfall to pull that for us. Everything he had was printed, because they don’t allow flash drives, laptops or mobile phones inside Biham and Associates offices. He printed everything that night and when he got out of the building, he asked us to pull him out, because he had been burned.”

"Hmm," Richard murmured. He had always emphasized to the team the importance of adhering to OPSEC regulations even in cyber operations. Sending that phish could have immediately burned Chematstone.

“We agreed, and a team was to exfil him out near the border town to Tigray, because it was easy for him to pass as a local or even as a refugee, that’s after the meeting for a brush up inside Bole International Airport. It was a long shot. Both men executed the rendezvous, on Friday afternoon and that’s when we lost him, and LT Nyalita was KIA at the scene.”

“Sir.” Captain straightened his jacket and asked. “Has LT's family been informed? Sir.”

“Captain!” The Brigadier snapped. “Cool it down.”

Richard recalled the Major was away. The Captain, who was supposed to be in charge, didn't seem ready.

“Focus up.” The Brigadier roared. “I need your team battle-ready for this op. All arrangements on Lieutenant Nyalita's transpo, and everything will be executed by another team. We have a national security event on the horizon."

The Captain lowered his voice. "Sir."

"Okay." The Brigadier pointed at Colonel Cyber. "Lets proceed."

Richard saw the Captain equivocate. His eyes had turned red.

"Sir." The Colonel replied and picked up from where he left off. "Before Chematstone disappeared, he had given us information, that something had happened during the exchange of the cargo at the warehouse, and one of their employees, a Kurdish or a Syrian, had seized one of the boxes. Then he ran and disappeared with it out of Biham's warehouses guns blazing. Intelligence suggests south of Addis Ababa."

The Brigadier nodded to allow him to carry on. His clenched fists indicated he knew, that there was no doubt whatsoever, that the package had made its way through the border, and into northern Kenya.

"His name, —er, is Bashir. A.K.A. Akhil." Colonel Cyber paged some photos and a report over the files. "Probable real name, Rushdi Al-Azmah. So, the whole intel shop has been digging throughly on him. He is a probable Al Qaeda hardliner. Everything has been kept under the rug to avoid the media breaking the news."

Richard understood that the only reliable aspect of the media was its unreliability.

"So. After he stole the case, Biham and Associates mercenaries pursued him into a town South of Addis Ababa called Negele. Then, there was a deadly shootout inside a hospital, and several civilians were injured."

Richard wondered how they kept that under the lid.

Colonel Cyber continued. "Bashir disappeared thereafter, into a plantation nearby and we can only assume he is in the country. He had backup probably an Al Shabab QRF. We assume it's another unit of Amniyat stationed inside Ethiopia. He could have penetrated into the country through Sololo or Laga because Moyale is heavily guarded."

The Ethiopian-Kenyan border was porous. It's known that many Tigrayans started crossing over when the fighting began in Northern Ethiopia.

"So." Colonel Cyber leaned back in his chair. "Whatever he is carrying could be life-threatening, beyond our comprehension. We have to intercept at all costs."

Richard tried to remember the Northern Kenya map. Laga was connected through a large forest known as Turbi Forest from Ethiopia. He couldn't picture where Sololo was. It had been years since he visited that part of the country. If Bashir was a hardened and trained Jihadi, he would find his way through the woods. That border was not a real border.

Richard dreaded the next part.

The Captain sat defiantly. His legs were spread and his hands curled into fists.

“Okay.” The Colonel had paused and was spreading more of the papers on the table. He pulled a target package folder that had another name on it. “So far, predications from National Intelligence Service show, there could be a connection to a radical Syrian national in Eastleigh, whom they have been watching for a while. Bassam Al-Salek.”

Richard considered the Human Intelligence aspect during counterterrorism. NIS was proficient in HUMINT; they were the best in Eastern Africa, even though HUMINT collection is more susceptible to dilution than cyber.

“We had requested November to exploit any laptop or mobile device on target, but there was no success.”

They were all aware of November’s inadequate cyber capabilities. They always fortified their position through the acquisition of fear, policy, and deception.

Colonel Cyber said. “We cannot believe or run workups on these predications that these guys always give us. Sir, we require data and intelligence instead of thesis on this matter, to avoid blow back from the local Islamic community.”

“Understood.” The Brigadier acquiesced. “The General and I have put that into consideration.”

Adversaries were using highly secured systems, and some had even switched to Linux and Apple devices. Having no evidence on a well-known cleric would be catastrophic for the senior officials signing off on the operation.

“I see.” The Brigadier paused. He seemed to reflect on it for a minute. Then he said. “Proceed.”

“Thank you sir.” The Colonel turned to another report that had high level classifications of Sensitive Compartmented Information, SCI. “Sir, the Recce team and our assault team will be on the ground at Eastleigh to take him tonight.”

Richard looked at Brigadier Thuo. Judging from his expression, he was determined to have this guy grabbed. The Counter Terror intel shops wanted him too. For a moment he hoped, that there would be no pissing contest.

Colonel Cyber added. “As DoD we don’t have jurisdiction inside Nairobi, so Recce will have to go in first, sir. They will take the lead. Their Recce commander will be on point as a deconfliction asset with our Alpha group commander. Michael Lisudza.”

"Roger that." The Brigadier affirmed. He then queried, "Assault team will be with them outside to relay information, right?"

"Yes sir. Plan B." The Colonel told him. He picked up another folder. "Plan Bravo will be cyber, if Bassam interrogation doesn't bear any fruits. We activate cyber. And this is where Richard and Captain come through."

At this point, Richard knew that they were using cyber as a backup plan rather than a shaping operation's asset. However, for all intents and purposes, it would be employed for covert action against Biham and Associates.

The Brigadier said. "There is a significant political component on how we respond. Every government around us is watching what we will do next, and what the Ethiopians will do."

The Captain was unusually quiet, as if preoccupied.

"Captain." The Brigadier asked, "Can we have the screen at the training area, wired and connected with the SWCADG's Assault team?"

The Brigadier was referring to a tier one assault team, which was closely integrated with the DMI's covert intelligence unit, commonly known as SOG due to the acronym's pronunciation. *Saawkgee.*

"Sir?" The Captain asked startled. His mind was somewhere else.

"Captain. I know LT. Nyalita is a family friend." The Brigadier paused, waving away any response. "But."

Richard knew he was about to tear him a new one.

The Brigadier stood up and briefly rested his hand on the Captain's shoulder. "Let's figure out what happened, and then we deal with them. All of them. For L.T. So that he can rest in peace. Knowing we avenged what they did, he will rest. *How-do-you-copy*?"

"Yes sir. Copy that sir." Captain Mwangangi snorted. "I agree with you sir. I am with you. One hundred percent sir."

Brigadier Thuo quickly moved on. He wasn't ready to give an impromptu therapy session.

Richard quickly figured that those were for his daughter.

"Gentlemen." Brigadier's inner leadership had taken over. "Then, it's a go. Get them gentlemen."

CHAPTER EIGHT

Too many operations often derail increasingly, because of friendly fire.

SWCADG, aka MadDog SOG1, Alpha Team's lead head-cam, streamed to the screens on the DIA's hall above the training library. The library had been closed off for the month due to renovations, but it was a cover. Alpha team lead said, "This Alpha One."

The Captain was the one on the radio relaying back. "Go for CFOB, Alpha One."

The students were back on their desks which by now, were all rearranged into an operations center, currently codenamed Cyber Forward Operation's Base, CFOB.

The Brigadier and the Colonel Cyber were seated next to Richard as he struggled to get the Two terabyte hard-drive to work.

Alpha called back in. "Recce team is taking point. They are going into the target building."

The task-force had been staged a few blocks from where Bassam Al-Salek lived in Eastleigh.

The DoD had not granted clearance for the Special Operation Group's squadron, commonly known as SWCADG. The unit worked with DMI on CT operations due to their Assessment and Control experience on the homefront, despite the Brigadier's request to include them in the taskforce for battlefield interrogations. The DMI had demanded earlier on the call; 'This will bring a shit-storm to DoD if the public knows that the Special Warfare soldiers were there. NO! Let DCI and NIS handle this.'

Richard kept his eyes trained straight ahead at the screen.

The Colonel nodded at the Captain to go on, as he edged with the Brigadier at the main desk.

The Captain picked the radio and said. "Copy that Alpha. Make sure the CAM is facing the building. Is Recce relaying? Over."

"Roger CFOB," Alpha One replied. "We have comms with Recce team on a different channel."

“Copy that, relay back any intel from Recce.” Captain Mwangangi ordered.

“Good copy, sir.” Alpha One radioed back in. His breathing was heavy from running up the stairs to a staging front. “No HVT activity on target building. Recce has arrived and staging outside. I pass Baraka.”

“Roger that Alpha One. Baraka.” Captain answered the call and turned to a large paper behind him, which had DRC towns on the left as code names and specifications of each on the right. It was an execution checklist.

Aketi was ticked first for, IN POSITION WITH THE TASKFORCE.

The Captain ticked the next execution phase, Baraka. It was RECCE STAGED OUTSIDE TARGET BUILDING.

“—ck, yeah!” Richard groaned a heavily obscured curse from his desk. He was watching the ongoing op too.

Most of the men laughed at him to ease the tension.

Senior Sergeant Duncan's fist bumped Richard’s.

Richard plastered a smile onto his face when Brigadier Thuo threw him a glance.

“What?” The Brigadier stood up and walked over. “What have you found?”

“I think they used magnets. Disks are okay.” Richard explained. “But sir, for this magnitude of corruption, those magnets had to be really huge.”

“At Bole, there was a man in front of me with a big bag and two women, carrying the same large bags too. The women came to the restaurant I was in.” The Brigadier sat next to Richard. “That’s how they did it I guess. I was also wondering why they squeezed in together at the lift. I remember thinking it was just European tourists rushing for their Safari and I was sorry for them. But at the restaurant it was different. They were Russians. They spoke Russian.”

Richard wondered how they passed and cleared the airport checkpoints and then he remembered that if they were SVR, then they had support from some CNOers from Russia or assets at the immigration desk. All they had to do was to make the computers blink. Maybe display that the bags were full of clothes and shoes.

The radio in front quaked. “This is Alpha One. I pass Bandundu. Recce is inside the target building.”

“Copy that.” Captain ticked Bandundu, RECCE BREACHES THE BUILDING.

Richard observed the Captain return the radio to the cradle. The receiver had been rigged to resemble those old school hard-lines. He stared at the ancient-looking machine. Instead of a cord running from the back, there was a large red wire. There were no number keys except large blipping nobs. It was a specops Thales Group long-range tactical radio.

“CFOB, there is a fire fight. One military aged male pulled out an AK.” Alpha One reported back. “CFOB how copy?”

The Brigadier stood up. His hands were clenched. His eyes burned with fury.

Richard glanced at him. He thought how sideways this had gone. There was no plan that survived fast contact.

“Good copy Alpha One.” Captain Mwangangi called back. “Interrogative, any one down from Recce?”

“Negative CFOB. Two enemy combatants are down hard now. Search for HVT is ongoing.” Alpha One relayed out. The Colonel stood up too and some of the students started approaching the main screen.

The Colonel asked the Captain. “His phone is still there?”

“Yes sir, the signal was live 30 minutes ago.” The Captain explained. “We expected some resistance. Two Tango Kilo. Dry hole, not confirmed. With such resistance, he is there. Expecting photos from Alpha Team, for facial-rec and confirma —”

“SVEST!” Alpha One came back on radio. “SVEST! SVEST!”

Richard stood up like on cue. He turned his attention to the big screen. The serious and engaged cyber classroom seemed like a lifetime ago.

Captain Mwangangi picked up the radio’s cradle, “Say again, Alpha One.”

“SVEST in target area, stand by. Recce team is trying to clear the floor, over.” Alpha One replied. He then yelled. “Kinshasa — ”

There was a blinding light on the screen, and then a command prompt; CONNECTION LOST.

The Brigadier =========>

ABOUT THE AUTHOR

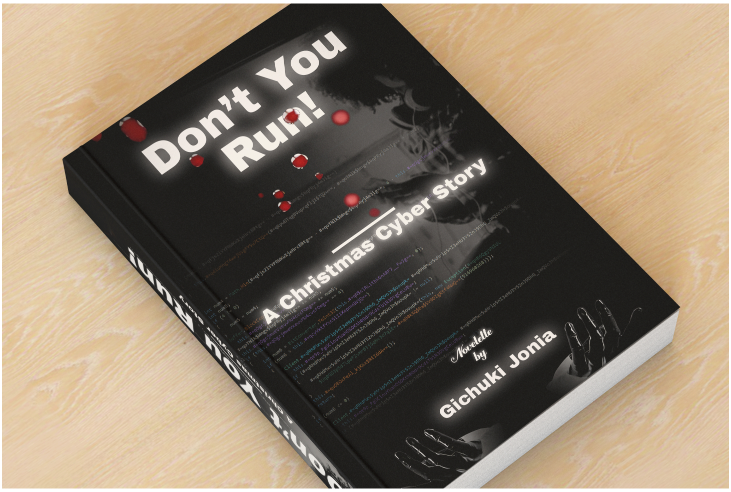
Gichuki John Jonia (Chucks) is a veteran cyber operator.
He is currently the CEO, OnNet Group.
https://onnet.group
He is an Author at CJBL and the Military/Intelligence Cyber Range Designer at CyberRanges.
He has worked in different regions running offensive cyber and defensive operations for Governments and other organizations.

His stories come from his time in the trenches fighting bad guys and defending large infrastructures.
He will be writing new books and their series in the coming years.
For more on the books check out https://chuksjonia.com/blog.html

In this novella, he takes you to the world of information domain as a support element of other domains in meatspace operations.

C0nn3ct B4ck is his second book, which is part of a new series known as the Ark Cyber Series and dubbed as C0nn3ctB4ck Series. The book was divided into two parts to meet the word count. The first part is known as '**The OJT**,' and the second, which is a larger novel, is known as '**Operation Frozen Trees.**'

ALSO BY GICHUKI JONIA



DON'T YOU RUN
A Novelette

He always watched them. They were his victims …

BROKEN HEARTS:

It's Christmas, and Paige Mwangi is still a heartbreaker. Boys at school have always loved her, but they never could get to her. She has always played the role of the spoiled, rich, beautiful girl. Then, the worst happened last year when a close friend offered her up to a gang of school boys. She changed schools and started a new life, but the worst still followed her.

THE CREEPER:

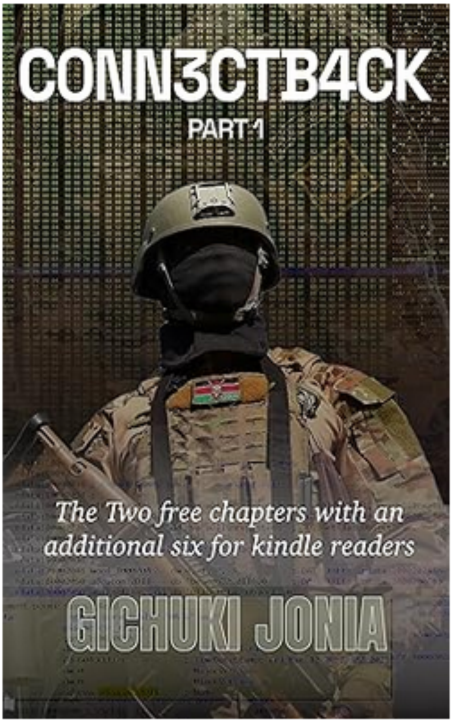
Her lure crosses paths with a dangerous serial killer and rapist. A serial Predator.
Through Paige’s father's company, her laptop and devices are hacked. This man is able to watch her remotely because that is exactly how he observes his targets before striking.

INVESTIGATIONS:

Vic is able to find out that some tactics, techniques, and procedures used inside Paige’s father’s company are not just from a local African Financial Threat, but another threat actor is inside their systems and is targeting both Paige’s laptop and her father’s. The killer is much more brilliant and uses sophisticated tooling. After this killer targets Paige, the next thing left is he kidnaps her just like he did with the other girls. But he is escalating on his hunts and kills.

TIME IS RUNNING OUT:

He doesn’t keep a girl for more than three days. He will ask for some payment, which is usually a ruse because he eventually doesn’t honor it. Vic and his partners have to help the DCI reach her and rescue her, but time is running out. None of the victims survived so far. None of them returned home.


CONN3CTB4CK
PART 1
The Two free chapters with an additional six for kindle readers
GICHUKI JONIA

C0NN3CTB4CK - Part 1 Free Chapters

A compromised asset, a cyberops class, and a counter-terror operation gone awry

A Novelette

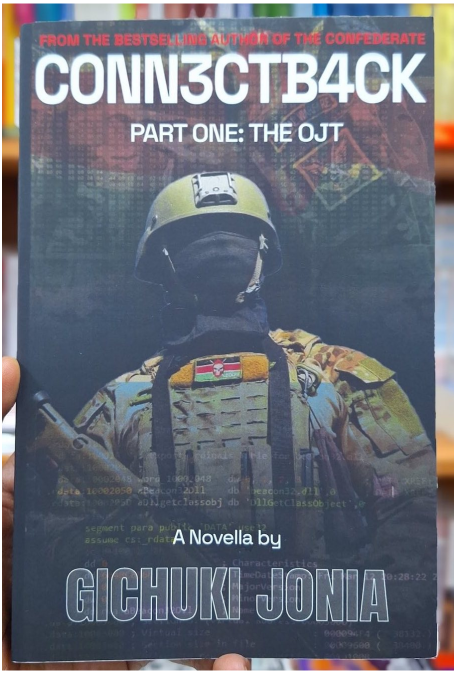
A Lieutenant is pulled from an active counterproliferation mission in DRC, November 2021, for a brush-off operation in Addis Ababa. A Directorate of Military Intelligence asset, plans for that brush up with the Lieutenant at Bole International Airport, Ethiopia.

There is gunfire at the airport and the LT is clipped during that meet. The Asset is on the run back to Tigray.

A Brigadier is surveilled by foreign counter intelligence operatives as he flies back to Kenya from Ethiopia. An S-Vest goes off in Eastleigh during a Counter Terrorism operation.

An Offensive Cyber Operation is under works.

An entity is ready to deploy destructive cyber tools against a vital Kenyan Diplomatic and Intelligence station.



C0NN3CTB4CK - ON THE JOB TRAINING

A cyber war class, a terror raid, the Tigrayan war

A Novella

Following the directive for on-the-job training (OJT), Richard and Anthony find themselves in Ethiopia, carrying out Operation Angel Wings. Meanwhile, the disappearance of Gebre, codename Chematstone, raises concerns for Brigadier Thuo, who urgently needs him located.

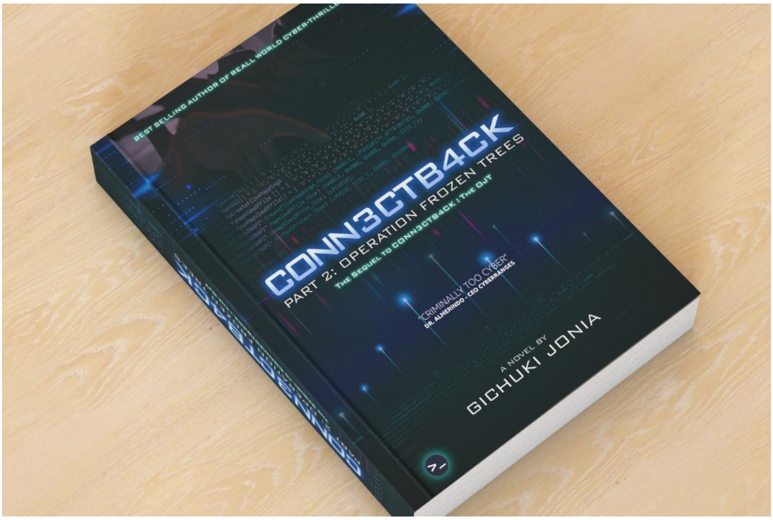
With the presence of a potential traitor within their circle of trust, will Richard and Anthony successfully accomplish their mission's end-state?

<u>IT WASN'T OVER</u>

Chinese information operations doctrine, Vulnerable weak Nations, Gold, Lithium, Oil

A Novelette

Compromised by the Chinese MSS after joining the Kenyan National Intelligence Service's OCNO, Josh's love of money drags him deeper into the claws of a foreign intelligence service running ops to counter NATO and US influence in East-Central Africa — until someone tries to take him out in the supposed safety of his home.


BEST SELLING AUTHOR OF REALL WORLD CYBER-THRILL
CONN3CTB4CK
PART 2: OPERATION FROZEN TREES
THE SEQUEL TO CONN3CTB4CK : THE OJT
"CRIMINALLY TOO CYBER"
DR. ALMERINDO - CEO CYBERRANGES
A NOVEL BY
GICHUKI JONIA
>_

C0NN3CTB4CK - OPERATION FROZEN TREE

A compromised operation. Several hunters. Tigrayan war

A Novel

As Gebre tries to escape Addis Ababa amidst the raging war in Tigray, Richard and Anthony's counterintelligence and counter-cyber operation at the embassy goes awry, forcing Anthony to flee. Brigadier Thuo launches an extraction operation for the high-value individual (HVI) Gebre (Chematstone) from Ethiopia, deploying a highly classified Tier One unit working directly for the Military Intelligence. Richard is tasked with supporting the team on the cyber front for the CFOB activation, where Meatspace meets Cyberspace.

With all these moving parts, will the teams achieve their objectives and counter the threat actors that are active and against them?

Will Anthony and Richard make it out of Ethiopia safely?

Will they figure out who the mole is?

And will they sniff out the mole at the Embassy?

This book is dedicated to the Tigrayan children who lost their lives and those whose lives were forever altered by the conflict.

It is also dedicated to our brave brothers at the frontlines fighting in the ongoing conflicts and to those who have made the ultimate sacrifice, allowing us to enjoy the freedom that we may not fully comprehend or deserve.