



Red Diamond

Contemporary

Operational Environment

and Threat Integration Directorate

Fort Leavenworth, Kansas Volume 1, Issue 1 NOV 2010

Army TC 7-100: Hybrid Threat

SPECIAL ITEMS:

- New Hybrid Threat doctrine TC 7-100
- New Exercise Design TC 7-101
- OEA 5: Iran
- Common Framework of Scenarios (CFoS) explained
- INFOWAR article
- New TRADOC G2 Handbook No. 1.08 (Revised FNL DRF)

On 29 Oct 10, TRISA-Threats forwarded the final electronic file of Training Circular (TC) 7-100 through the Army Training Support Center (ATSC) to the Army Publishing Directorate (APD) for publication in electronic media only. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually beneficial effects.

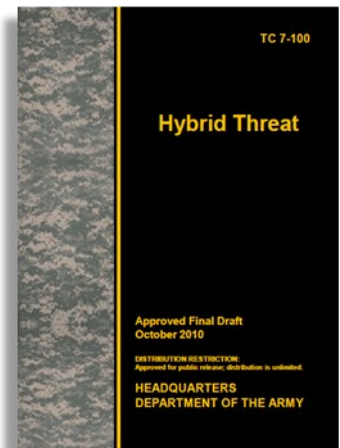
The purpose of this TC is to describe hybrid threats and summarize the manner in which such threats may operationally organize to fight U.S. forces. TC 7-100 also outlines the strategy, operations, tactics, and organization of the Hybrid Threat that represents a composite of actual threat forces as an opposing force (OPFOR) for training exercises.

When published, this TC will supersede FM 7-100, *Opposing Force Doctrinal Framework and Strategy*, 1 May 2003. As an interim measure, TRISA-Threats has posted the current version on its AKO website at :

<https://www.us.army.mil/suite/doc/25291910>

After Army authentication, APD will post this TC on AKO/ Self Service/DA Pubs & Forms/Doctrine and Training Publications.

- (<https://akocomm.us.army.mil/usapa/doctrine/index.html>) ,and
- ATSC will post it on the Reimer Digital Library (<http://www.adtdl.army.mil>). All these websites require AKO login.

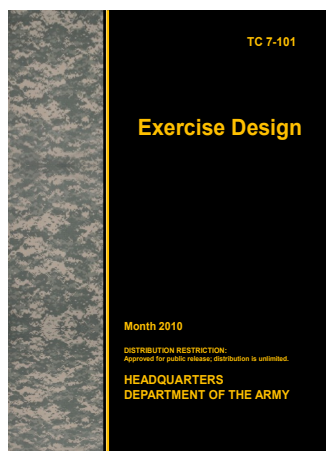


HOT Topics:

Inside this issue:

TC 7-100	1
TC 7-101	2
OPFOR Doctrine	3
Irregular Forces	3
TTP	5
INFOWAR	6
CTID SMEs	8





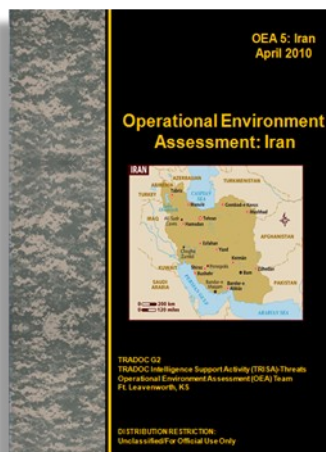
Army TC 7-101: *Exercise Design*

On 29 Oct 10, TRISA-Threats forwarded the final electronic file of TC 7-101 through the Army Training Support Center (ATSC) to the Army Publishing Directorate (APD) for publication in electronic media only. This TC outlines a methodology for designing and executing training exercises. It describes planning procedures and methodologies, responsibilities, and analysis for those who plan and control Army exercises across all training domains and environments. It also provides exercise planners the tools necessary to create realistic and challenging exercise conditions in order to support the unit's training objectives and effective training. Procedures and tools outlined in this TC are intended to be applied across the entire spectrum of conflict.

As an interim measure, TRISA-Threats has posted the current version on its AKO website at: <https://www.us.army.mil/suite/doc/25292460>

- After Army authentication, APD will post this TC on AKO/Self Service/DA Pubs & Forms/Doctrine and Training Publications at: (<https://akocomm.us.army.mil/usapa/doctrine/index.html>), and
- ATSC will post it on the Reimer Digital Library at: (<http://www.adtdl.army.mil>). All these websites require AKO login.

Operational Environment Assessment

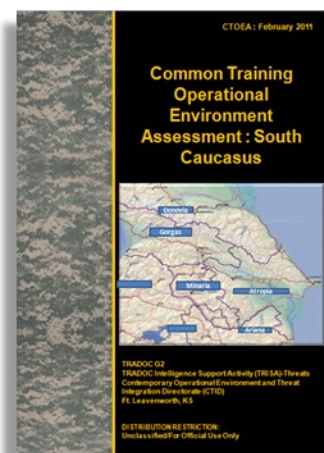


CTID's Operational Environment Assessment (OEA) Team recently produced an update to the Iranian OEA. This real-world OEA presents a detailed analysis of the political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) variables as they relate to the operational environment (OE) of Iran. This OEA can be used for training events, cultural awareness instruction, and scenario development. Other completed OEAs include: **Iraq, Afghanistan, North Korea, Azerbaijan, the Horn of Africa (HoA), and Pakistan.**

Coming Winter 2011!

CTID is currently developing a Common Training Operational Environment Assessment (CTOEA) for the South Caucasus. This CTOEA will present a common fictional OEA for training against actors across this region. The CTOEA will be used across all Combat Training Centers (CTCs)/power projection platforms/exercise divisions. The CTOEA is not a scenario.

CTCs still write their own scenario, but after the publication of the CTOEA all CTC scenarios for full spectrum operations will be written utilizing conditions highlighted in the CTOEA. Publication date for the first draft is set for February 2011.



<https://www.us.army.mil/suite/doc/22050545>

Opposing Force Doctrine

Forthcoming Publications

TC 7-100.2, *Opposing Force Tactics* will be published in the spring of 2011. When published TC 7-100.2 will supersede FM 7-100.2, *Opposing Force Tactics* dated September 2004.

TC 7-100.3, *Irregular Forces* will also be published in the spring of 2011. When published, TC 7-100.3 will supersede FM 7-100.3, *Opposing Force: Paramilitary and Nonmilitary Organizations and Tactics* dated February 2002.

TRADOC G2 *Worldwide Equipment Guide* will be published in December 2010. The OPFOR Doctrine Team (ODT) develops opposing force (OPFOR) doctrine used to set the conditions in all U.S. Army training, education, and leader development venues (live, virtual, and constructive). OPFOR doctrine supports all aspects of full spectrum operations. This doctrine is developed by incorporating relevant real-world threat and enemy military capabilities, equip-

ment, organizational structures, and TTP. OPFOR documentation may be disseminated in the form of the FM/TC 7-100 series of field manuals/training circulars, guides such as the *Worldwide Equipment Guide*, or as a series of short articles designed to inform trainers and Soldiers about relevant threat TTP or equipment.

Some examples of products produced by the ODT are: FM 7-100.4, *Opposing Force Organization Guide*; 2009 *Worldwide Equipment Guide*; TRADOC Handbook No. 1.08, *Irregular Forces*; TRADOC Handbook No. 1.07 C2, *A Soldier's Primer to Terrorism TTP*; and the TRISA War on Terror Poster No. 01-11.

ODT projects currently in production are: TC 7-100.2, *Opposing Force Tactics*; TC 7-100.3, *Opposing Force Irregular Forces*; 2011 *Worldwide Equipment Guide*; Review of AMSAA proposed MILES PH/PK data; Review of WARSIM RISTA data; Military Variables and Orders of Battle for the CTOEA; and WARSIM data scrub review to BCTP Parametric Database.



All CTID products can be found on AKO. Check out all of our products at:

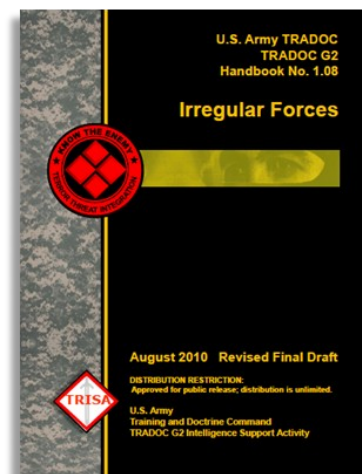
<https://www.us.army.mil/suite/files/11318389>

Threats Terrorism Team (T3)

TRADOC G2 Handbook No.1.08 *Irregular Forces*

TRADOC G2 Handbook No.1.08, *Irregular Forces* describes contemporary irregular forces and summarizes tactics and techniques confronting the U.S. in the current OE. By improving situational awareness and understanding of real-world capabilities, limitations, and intentions of irregular forces, this handbook complements the deliberate processes of military risk management, antiterrorism awareness, protection of the force, mission orders conduct, and adaptive decisionmaking in crisis venues by U.S. Army leaders.

Persistent conflict by irregulars will normally be indirect and asymmetric; however, irregular forces can be integrated into a full range of military and other functional capacities such as politics, social welfare, religious ideologies, economic programs, and regional or global media affairs. Ultimately, irregular forces will promote strategic concepts, conduct operational actions, and execute tactics to obtain influence over a targeted population and enhance legitimacy for their organizational objectives. Contemporary irregular force patterns and trends indicate how irregular threats might act in future near and mid-term conflicts against the U.S.



TRADOC G2 Handbook 1.08 will transition to a new Training Circular 7-100.3, *Irregular Forces*, with a publication date to be determined in 2011.

<https://www.us.army.mil/suite/doc/25258023>

Professional Military Education

Frequently Asked Questions/Concerns about the Common Framework of Scenarios (CFoS) web portal at: <https://tradoccommonscenario.army.mil/>

1. What is the purpose of the CFoS web portal?

The CFoS Directory is a repository of resource information of Common Framework approved scenarios for training, education, leadership, and capability development.

2. I am a first time user and after clicking on the web link I am directed to a screen with a box with a tab "NANW." What do I have to do to gain access to the web portal?

The CFoS web portal requires a valid AKO/DKO account or CAC card. From the ADFS realms page select AKO SSO from dropdown list and click the "Submit" button. Once on the web portal you will have general read-only access to CFoS portal. Scenario Developer or Member access is available by using the Service Request form under Help Desk or contacting the Portal Administrator.

3. What is the foundational directive and where can I find it?

The 3 February 2010 FRAGO 19 to OPFOR 09-008, TRADOC Campaign Plan contains the CSoF directive. Currently the task or challenge for TRADOC Centers of Excellence (CoE) and Schools is to replace any non-Scenario Board of Governor's (SBoG) approved scenarios with an approved scenario from the CFoS Registry to support Branch specific training.

4. Currently some proponent schools use terrain walks in local areas surrounding their installation to conduct training for their soldiers. How can we continue this activity and ensure compliance with the CFoS?

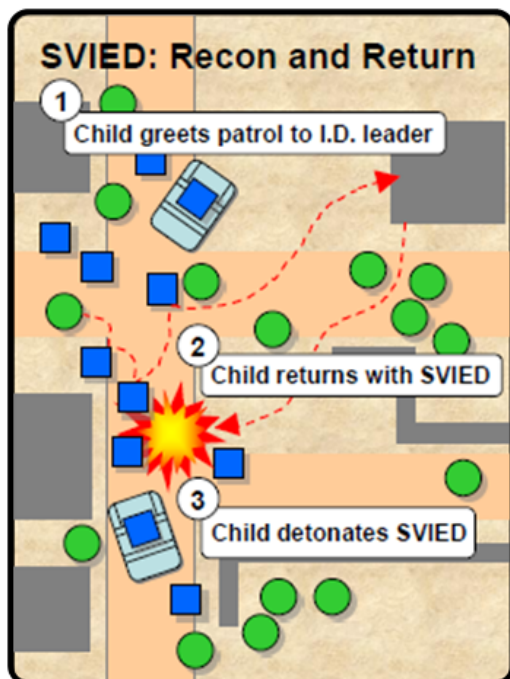
What you are referring to here is the use of a situation or vignette for a "Practical Exercise" to reinforce a learning objective. There are some CONUS terrain based scenarios within the CFoS registry that could be adapted for use by the training, education, and leader development community. For example, the Full Spectrum Capability Multi Level Scenarios (MLS 1.0 and 2.0) could be tweaked or adapted for use by a school to meet the desired learning objectives. Thus, you could still use local terrain to meet or be in compliance with the CFoS directive.

5. If we need to tailor one of the approved scenarios to meet the Commandant's desired outcome how do we obtain approval for this action?

This question is answered in two parts. First "tailoring" is considered as taking an existing approved scenario and using or extracting portions of the scenario to frame the requisite conditions to meet the desired learning objective. Currently, a school is permitted to extract a portion or portions of a scenario to set the conditions for a desired learning objective, or what is commonly referred to as a vignette. The key is for the training developer to maintain an audit trail of what they changed and why they changed it for the vignette. For example, TRISA-Threats had one school contact us about a problem where they did not have enough Brigade Orders to meet one of their desired learning objectives. The school contacted the scenario proponent and detailed the potential shortfall. They are working together on a "fix" to accomplish the desired learning outcome.

Part two of this answer discusses the direction for those scenarios not meeting desired learning objectives. Paragraphs 4i and 10 of the CFoS Directive provide the direction for scenarios existing in the CFoS that does not meet the respective Commandant's desired learning outcomes. The Commandant can approve a "derivative scenario" for use at the school or CoE. First, a letter (signed by the Commandant) has to be submitted to the Scenario Advisory Work Group (SAWG) for review and consideration for submission to the Scenario Board of Governor's (SBoG) for approval. The letter outlines the requirements/gaps that require a new scenario to achieve the desired outcomes. The proposed scenario is reviewed by the SAWG to ensure that it meets the established OE criteria. Upon completion of the review, the SAWG will forward the "derivative scenario" to the SBoG for approval. Once approved, the "derivative scenario" can become a shared common scenario that is located on the CFoS Registry.

Tactics, Techniques, and Procedures (TTP)



SVIED: Recon and Return

Could this happen to YOU?

1. Children, women, and men have used this attack technique. The **bomber** will mask within a crowd. An **observer** and a **controller** may be present too.
2. The suicide bomber can approach as a group or individual to **identify a critical target** such as a patrol leader in this scenario. Having confirmed the location of critical target, the individual goes away temporarily to acquire a **suicide vest improvised explosive device (SVIED)**.
3. The individual returns to target and **detonates**. The observer records immediate actions of patrol while the controller exfiltrates area.



Know the Threat

WE are at WAR!
on TERROR

Coming Soon...

Change 2 "Hip-Pocket" TTP Handbook 1.07

Handbook 1.08 "Irregular Forces"

TRISA

Fight Hard and with Discipline!

TRISA WOT Poster No. 01-11
TRADOC G2 Intelligence Support Activity
<https://trisa.bcks.army.mil> Terrorism

(Source: DOD Defense Imagery; MC2 Wriston)



All CTID products can be found on AKO. Check out all of our products at:

<https://www.us.army.mil/suite/files/11318389>

INFOWAR

Specialization and threat lifecycle in Computer Warfare

By Jerry England



This primer presents the **CONDITIONS** that U.S. Soldiers confront during close combat ground maneuver against an enemy. The intent is to improve our situational awareness- operational understanding of threats and how to achieve our mission success.

<https://www.us.army.mil/suite/doc/25258021>

Trends in recent information attacks show that the planning and deployment lifecycle is becoming more specialized and less dependent on computer experts. Tactical information attack teams can release malware by deploying pre-programmed exploit packages onto the enemy's networks in a variety of combat situations, from stability operations to full combat, without reliance on specific technical expertise. INFOWAR units will use agents and various social engineering techniques to elicit needed information to gain both authorization for and access to computer information systems. This form of fraud is designed to obtain credentials or information for system access and to establish an electronic beach head on the targeted system. These individuals will compile information obtained over time through a variety of operations to assist future information attacks.

Once access has been established, hackers will attempt to increase system permissions to the level desired to make an effective attack. The preferred method for launching information attacks is through remote access to the targeted network, which can occur from any location as long as the hacker has access to the system. In some cases an INFOWAR agent is used to gain physical access to the targeted system and will conduct an attack by loading malware directly into the system through a portable storage device, such as a thumb drive or a CD. The malware-whether it is a virus or a Trojan- is usually not developed by the individual who conducts the attack: these programs are developed or purchased from programmers who specialize in developing malware.

Programmers that develop malware have found an increase demand for their product from a variety of organizations from criminal gangs to government-sponsored INFOWAR organizations. The software they produce is combined into exploit kits complete with scripts on how to launch the program and how to target certain systems. Programmers sell their products as well as upgrades like any other software company. In some Hybrid Threat environments, the state has INFOWAR programmers who develop advanced malware products for military purposes. Technologists, who usually do not have the same skills as the programmers, are then able to take the information gained from hacker teams and fraud agents and develop target lists based on the types of computer warfare weapons available.

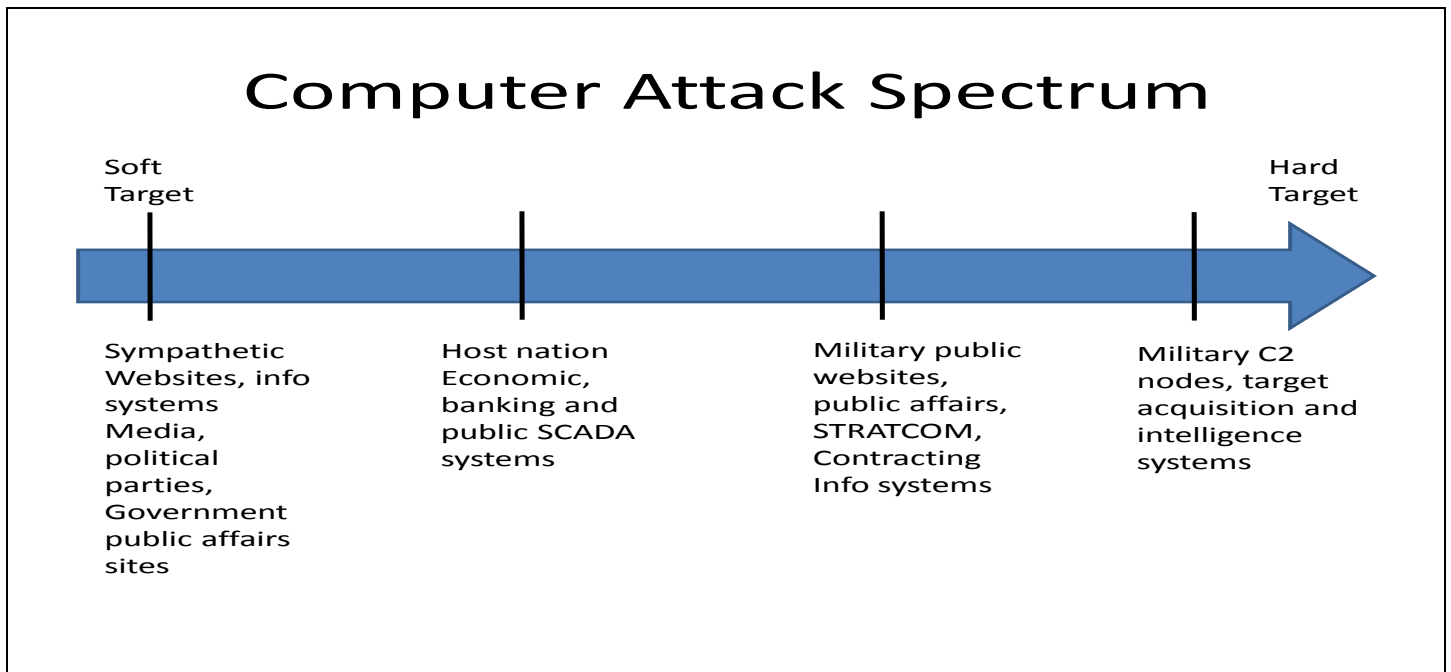
The targeting process is conducted by the INFOWAR intelligence management company and allows the commander to choose what systems to attack and how many computers to infect. The criteria are based on ease of access and the payoff associated with the risk involved. The potential payoffs for these operations are access to key intelligence about enemy operations; the ability to discredit the enemy through misinformation or defacement of public websites, or the ability to launch attacks designed to disrupt, deny, degrade, or destroy key enemy systems. Typical systems the INFOWAR units would target are C2 nodes such as net-centric warfare systems, intelligence channels, and sensor systems as well as public affairs and friendly local media outlets. Social networks also pose an increased threat to operations. Soldiers using free WiFi hotspots to check their personal social network page or personal email expose themselves to attack both from the network and from observation by trained INFOWAR agents.

INFOWAR

In some cases, a Soldier's personally identifiable information can be stolen and passed to criminal elements that steal Soldiers' identities causing personal problems at home and reducing a unit's combat effectiveness.

While many military C2 and intelligence systems represent "hard targets" due to the fact that they are "air locked" against information attacks and require multiple authorizations to obtain access, they are still vulnerable. Poor operational security, attacks from disgruntled employees or Soldiers, and lack of vigilance are avenues the INFOWAR units use to obtain unauthorized access.

In counterinsurgency and stability and support operations there are additional threats that come from the public nature of these types of operations. The fact that interaction with local populations is a key tenant of counterinsurgency makes automated systems that provide public information key terrain in cyberspace. The fact that these systems are available to the public makes them susceptible to vandalism or other information attacks like distributed denial of service attacks. The knowledge needed to conduct these types of attacks can be found on the World Wide Web and is a common, cheap means to achieve effects in INFOWAR perception management operations. Public information systems that tie directly



into military C2 nodes may offer yet another back-door vulnerability if the site is not properly administered. These systems represent soft targets in the cyber warfare spectrum.

As computer literacy increases organizations, and governments gain a variety of resources for conducting computer warfare operations. These types of operations are desirable because of the tradeoff between potential INFOWAR effects and relatively limited risk. Another key factor is that as global militaries rely more and more on communications systems that share large amounts of data and are integrated across all levels of command, the exposure to information attack increases. If there is a lapse in operational security at the edge of the battlefield, this exposes an opportunity to exploit that vulnerability. INFOWAR personnel who are trained to use social engineering techniques and hacking to gain access to computer systems will pose a significant threat in theater and can have damaging effects on operations.

YOUR Subject Matter Experts

Director, CTID DSN: 552
Mr Jon Cleaves FAX: 2397
jon.cleaves@us.army.mil 913.684.7975

OE & OPFOR Doctrine & Training Lit.
Senior Analyst CTID: Dr Don Madill 684.7926
donald.madill@us.army.mil

OPFOR Doctrine Team
SME: Mr Rick McCall 684.7960
rick.mccall@us.army.mil

Intelligence Specialist
SME: Mr Kris Lechowicz 684.7992
kristin.lechowicz@us.army.mil

Intelligence Specialist (Intern)
SME: Mr Jerry England 684.7934
jerry.england1@us.army.mil

Worldwide Equipment Guide (WEG)
SME: Mr Tom Redman BAE 684.7925
tom.redman@us.army.mil

Threats Terrorism Team (T3)
SME: Mr Jon Moilanen L3 MPRI 684.7928
jon.moilanen@us.army.mil

Operational Environment Analysis
SME: Ms Penny Mellies 684.7920
penny.mellies@us.army.mil
SME: Ms Angela McClain L3MPRI 684.7929
angela.mcclain2@us.army.mil

Training-Education-Leader Development
SME: Mr Walt Williams 684.7923
walter.williams@us.army.mil

National Training Center - OPFOR
SME: MAJ Terry Howard USAR 684.7939
terry.d.howard@us.army.mil

Joint Readiness Training Ctr - OPFOR
SME: Mr Marc Williams BAE 684.7943
james.marc.williams@us.army.mil

Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.spight@us.army.mil

Battle Command Training Program
SME: Mr Pat Madden S3 Inc 684.7997
patrick.madden@us.army.mil

Threats Website-Support Operations
SME: Mr Charles Christianson 684.7984
charles.christianson@us.army.mil

YOUR Easy e-Access Resource

AKO Three "Click" Drill-Down



Find Your Topic – Do Your Research

What We Do for YOU

- Determine OE Conditions
- Publish OE Threats in FSO
- Publish Army OPFOR Doctrine
- Assess Threat-Enemy & TTP
- Support Terrorism Awareness
- Publish OE Assessments

Director's Corner: *Looking Ahead --*

Our products are already available on the TRISA website, all you need is Army Knowledge Online (AKO) access. If you have identified a need in the areas of Operational Environments, OPFOR Doctrine, Weapon System Data, Hybrid Threat, or TTP, and you can't find it among our products, tell us!

<https://www.us.army.mil/suite/files/11318389>

Jon Cleaves