

Protecting Critical Energy Infrastructure: Design Basis Threat and the Cyber Threat



Presented by: Donald Dudenhoeffer



The Changing Face of Nuclear Security

Nuclear security is the protection of nuclear material, other radioactive material, associated facilities, and associated activities, including transport security. Nuclear security measures are designed to support the prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at such materials, facilities, operations.

- GATES
- GUARDS
- GUNS
- **GEEKS**



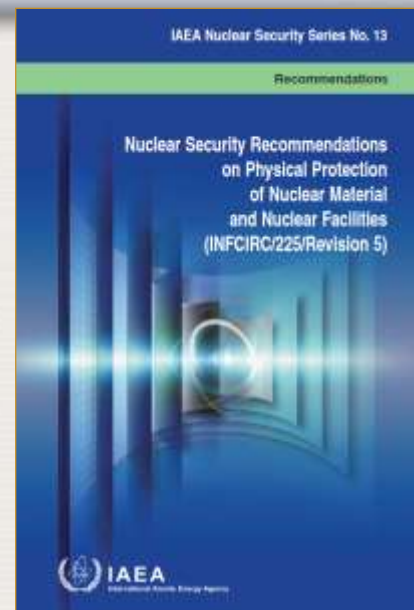
IAEA Role in Computer Security

Nuclear Security Series No 13 (INFCIRC/225/Revision 5)

“4.10/5.19 Computer based systems used for

- *physical protection,*
- *nuclear safety,* and
- *nuclear material accountancy and control*

should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat.”



The Threat – Adversary – Bad Guy

Most people have a hard time understanding the threat and thinking like the adversary.



Lone wolf?

Trusted Employee?



Dedicated group?

Definition of DBT

A Design Basis Threat (DBT) is:

- *a description of the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material, or sabotage, against which a physical protection system is designed and evaluated.*

Physical World – Well defined

Service history	
In service	1949–present
Designer	Mikhail Kalashnikov
Designed	1944–1947
Manufacturer	Izhmash
Number built	approximately 75 million AK-47 100 million AK-type rifles ^l
Specifications	
Weight	4.78 kg (10.5 lb) with a loaded magazine AKM weight with unloaded magazine 3.1 Kg.
Length	880 mm (35 in) fixed wooden stock 875 mm (34.4 in) folding stock extended 645 mm (25.4 in) stock folded
Barrel length	415 mm (16.3 in)
Cartridge	7.62×39mm M43/M67^l
Action	Gas-operated , rotating bolt
Rate of fire	Cyclic rate of fire is 600 rounds/min ^l Semi-auto rate of fire is 40 rounds/min ^l Full-auto burst rate of fire is 100 rounds/min ^l
Muzzle velocity	715 m/s (2,350 ft/s) ^l
Effective range	350 metres (380 yd)
Feed system	Standard magazine capacity is 30 rounds. There are also 10, 20, 40, 75, or 100-round detachable box and drum style magazines .
Sights	Adjustable iron sights with a 378 mm (14.9 in) sight radius: AK-47 has 100–800 meter adjustments AKM has 100–1000 meter adjustments



Impacts well understood

7.62×39mm		
Specifications		
Case type	Rimless, bottleneck	
Bullet diameter	7.92 mm (0.312 in)	
Neck diameter	8.60 mm (0.339 in)	
Shoulder diameter	10.07 mm (0.396 in)	
Base diameter	11.35 mm (0.447 in)	
Rim diameter	11.35 mm (0.447 in)	
Rim thickness	1.50 mm (0.059 in)	
Case length	38.70 mm (1.524 in)	
Overall length	56.00 mm (2.205 in)	
Case capacity	2.31 cm ³ (0.0356 gr H₂O)	
Rifling twist	240 mm (1 in 9.45 in)	
Primer type	Boxer Large Rifle	
Maximum pressure	355.00 MPa (51,488 psi)	
Filling	SSNF 50 powder	
Filling weight	18.21 gr	
Ballistic performance		
Bullet weight/type	Velocity	Energy
123 gr (8 g) Full metal jacket	731.5 m/s (2,400 ft/s)	2,073.6 J (1,529.4 ft·lbf)
154 gr (10 g) Spitzer SP	641.3 m/s (2,104 ft/s)	2,056.3 J (1,516.6 ft·lbf)
123.5 gr (8 g) Full metal jacket	804.7 m/s (2,640 ft/s)	2,460 J (1,810 ft·lbf)
123 gr (8 g) Full metal jacket	738 m/s (2,420 ft/s)	2,179 J (1,607 ft·lbf)
Test barrel length: 415 mm		
Source(s): Wolf Ammo ^[1] Omar ^[2] Sellier & Bellot ^[3]		



The Cyber Threat

How does one characterize the threat?

We can talk about Operational
Characteristics of computers



Processor

Intel® Core™ i7-2640M Dual Core (2.80GHz,4M cache,)

Operating System

Windows 7 Professional, No Media, 64-bit

Display

17.3" UltraSharp™ FHD(1920x1080) Wide View
Anti-Glare LED-backlit

Memory

4GB3 DDR3 SDRAM at 1333MHz

Hard Drive

750GB 7200rpm Hard Drive

Video Card

AMD® FirePro® M8900 Mobility Pro Graphics
with 2GB GDDR5

Optical Drive

8X DVD+/-RW

System Weight

7.77 lbs

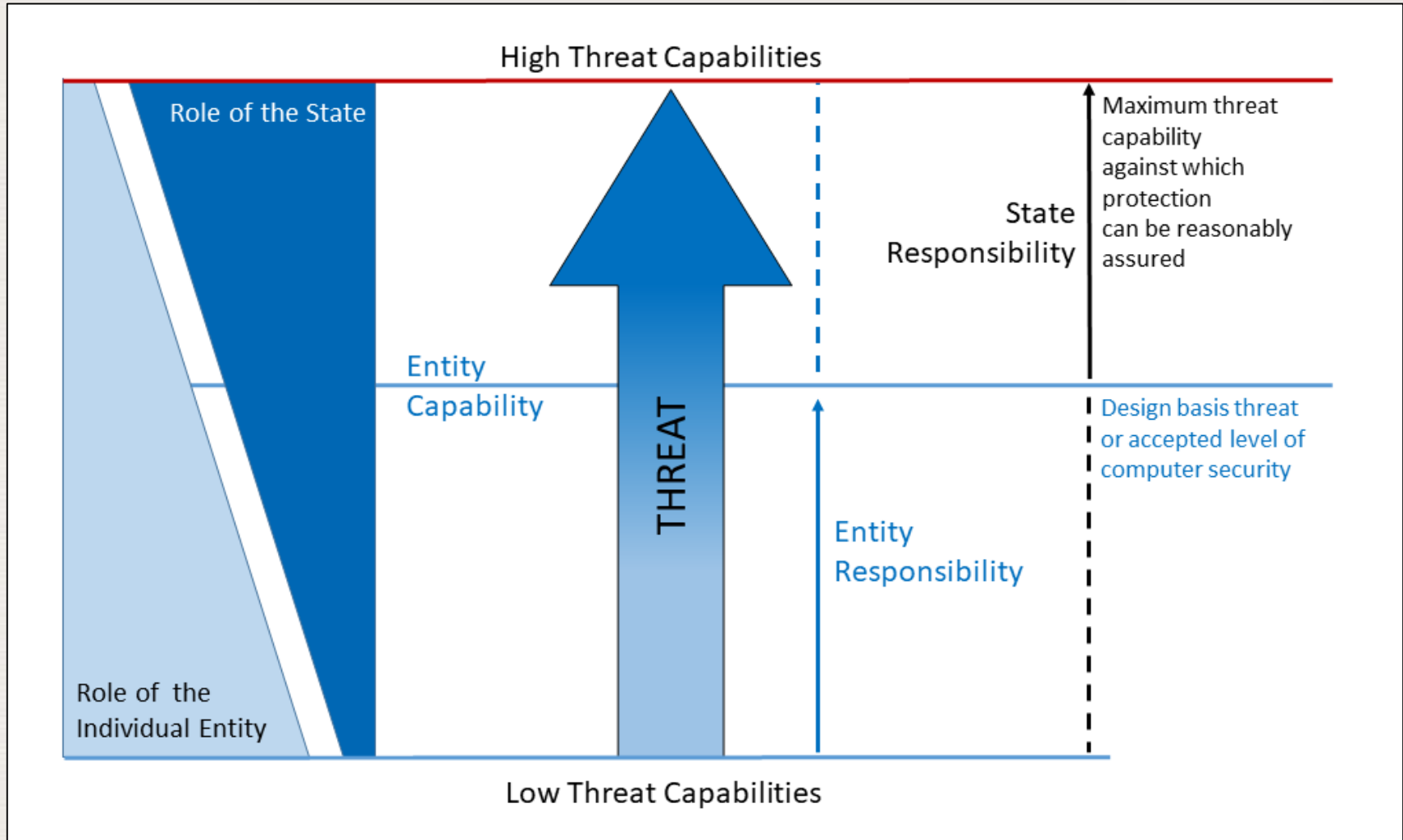
The Cyber Threat

How does one characterize the threat?

But how does one characterize the range of attack vectors – targets and methods, impacts?



Design Basis Threat



Questions?

