MARCH 2021

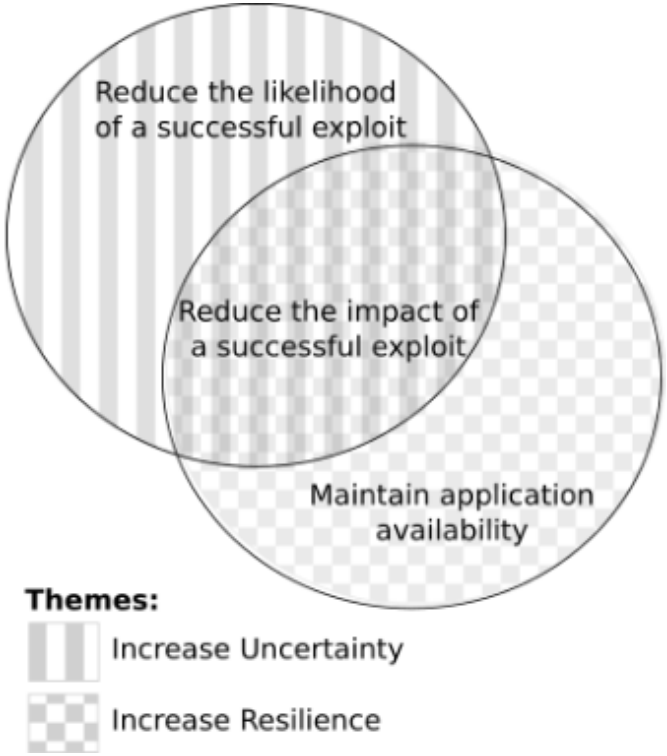
SS-MTD: STREAM SPLITTING MOVING TARGET DEFENSE

NATE EVANS, PHD, CISSP
SECURE Program Lead
nevans@anl.gov

Argonne National Laboratory's work was supported by the U.S. Department of Energy, Office of Science, under contract DE-AC02-06CH11357

Proactive Defense Focus – MTD 101

Two primary themes over three goals in proactive defense



MOVING TARGET DEFENSES:

BASED ON THE COMMON MISSILE DEFENSE TECHNIQUE

CHANGING SERVICES EVERY *N* SECONDS
SERVICE CAN BE OS, APPLICATION STACK, NETWORK DEVICE, IP, FIREWALL

EFFECTIVE ELIMINATION OF ZERO DAY EXPLOITS

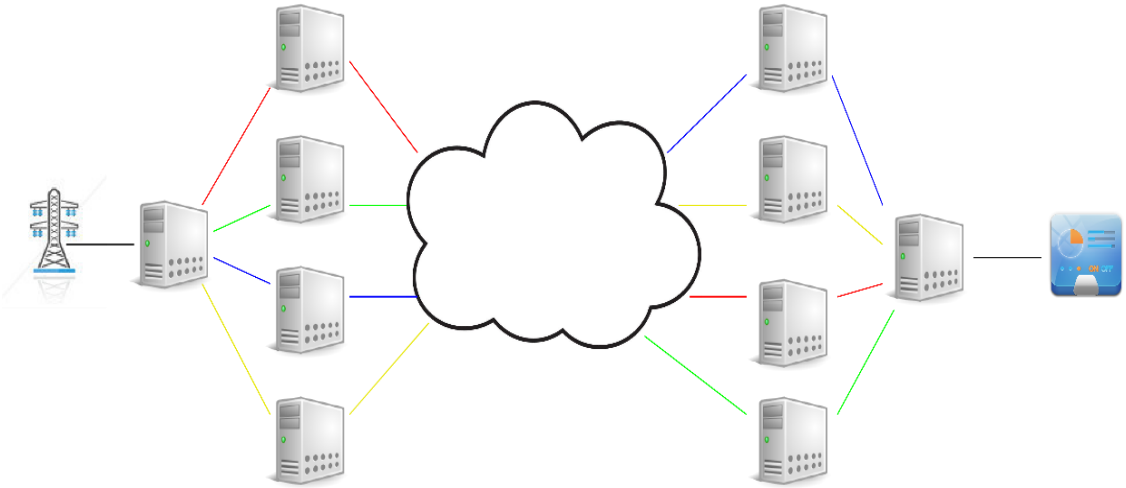
MULTIPLE MOVING ELEMENTS ALLOW VULNERABLE ELEMENTS TO BE REMOVED PENDING PATCHING AND QUALIFICATION / CERTIFICATION – OVERALL SYSTEM / APPLICATION STAYS UP ON UNAFFECTED PLATFORMS.

ROTATION ENVIRONMENT ALLOWS UPTIME DURING NORMAL OUTAGE EVENTS

QUARANTINING OF EXPLOITED SYSTEMS FOR FORENSIC ANALYSIS WITH ZERO DOWNTIME.
PATCHING, UPDATING, AND TESTING CAN BE DONE OFFLINE WITH UPDATED SYSTEMS ADDED POST CERTIFICATION WITH ZERO DOWNTIME.

MTD-STREAM SPLITTING

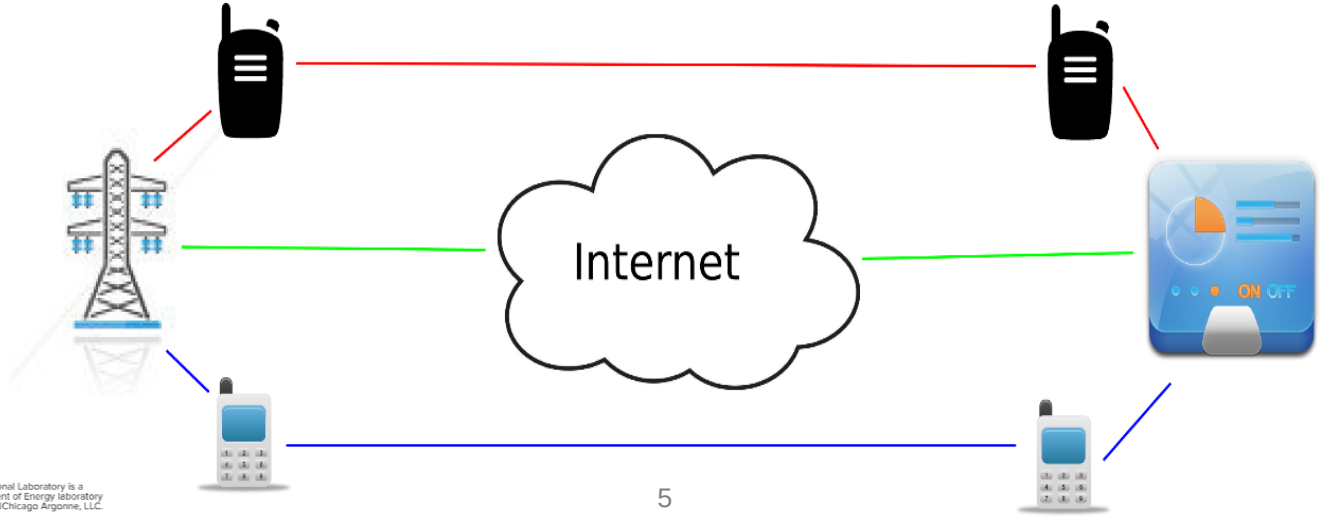
TCP stream splitting involves splitting a single TCP stream into many discrete units, sending and receiving those discrete units from and to different (ideally geographically disparate) receiving servers, with the stream being reassembled on the receiving end.

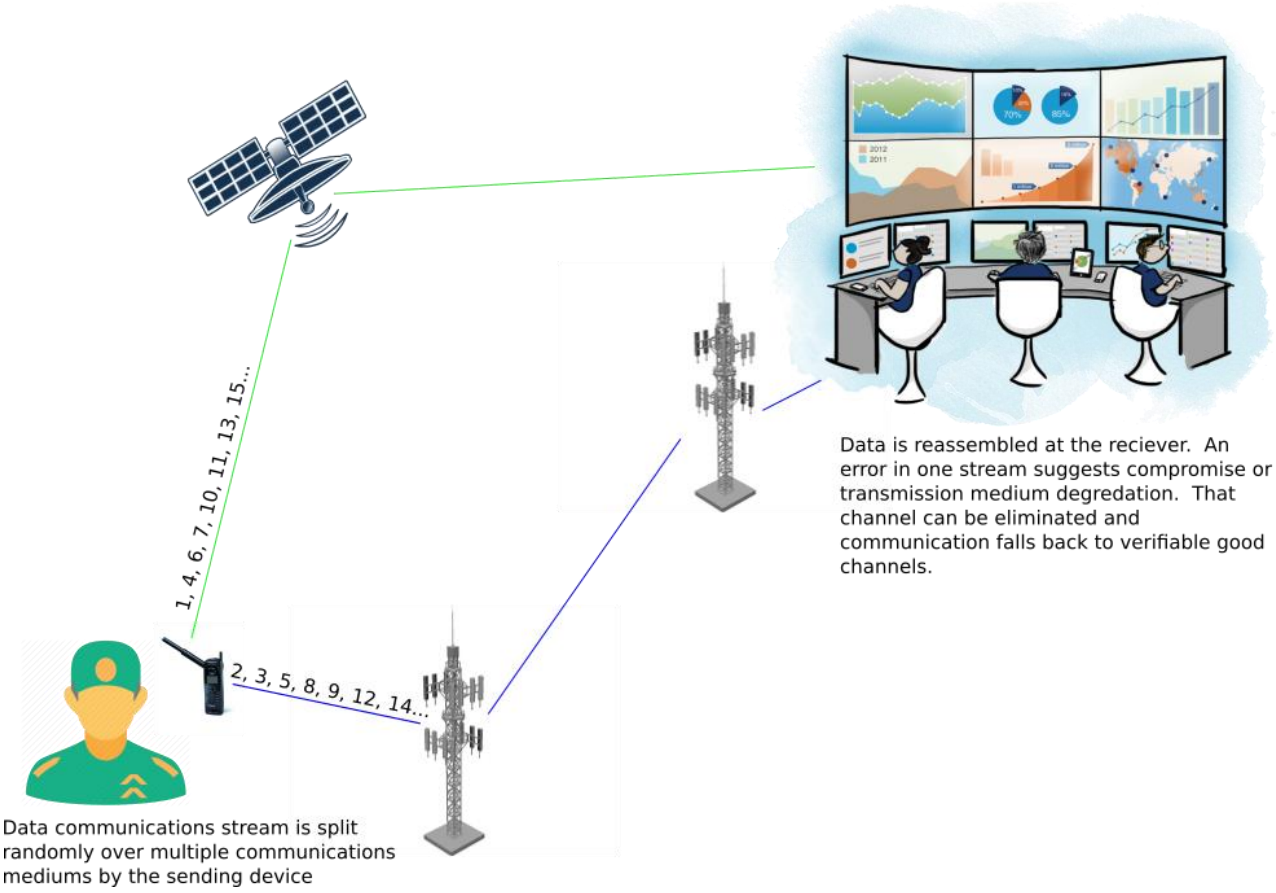


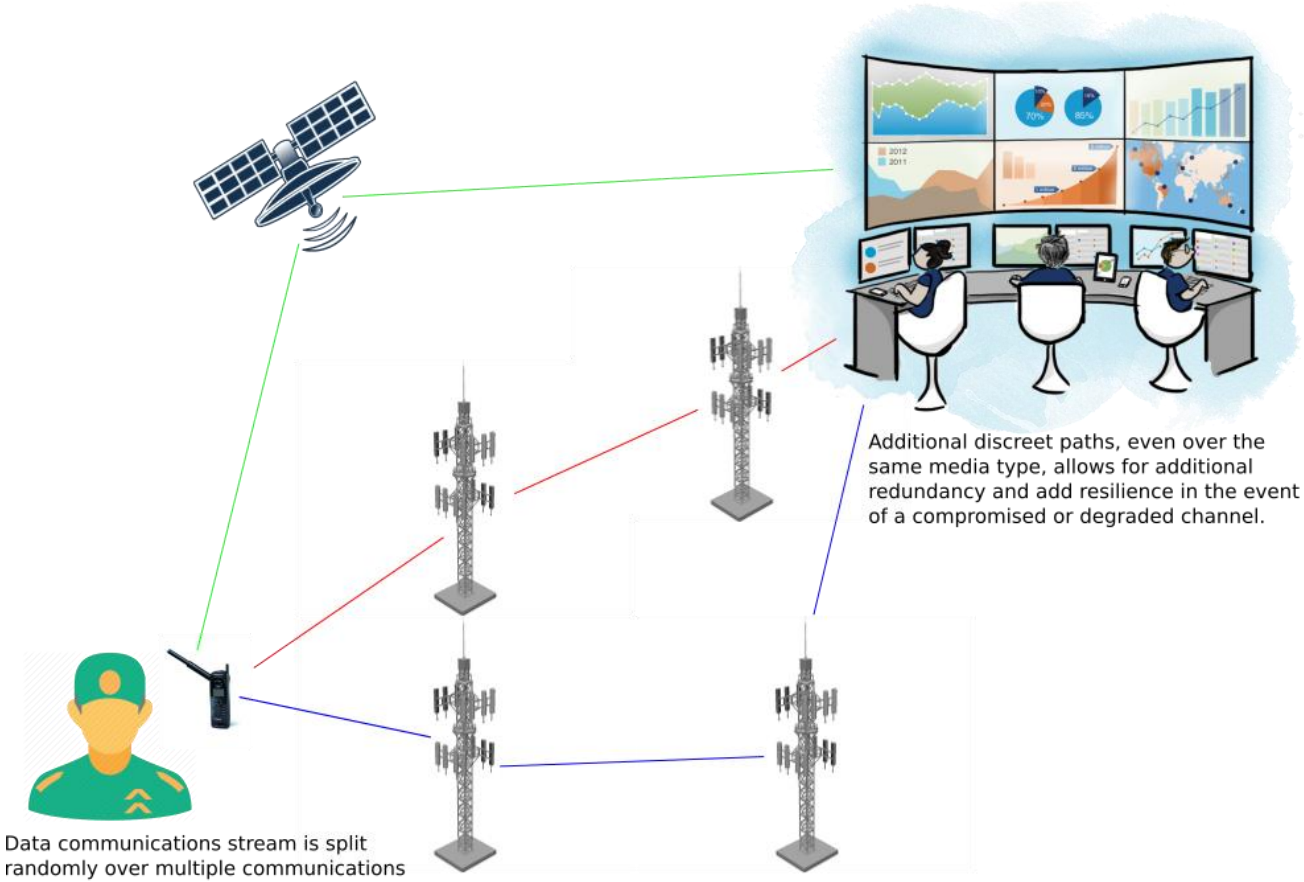
MTD-STREAM SPLITTING

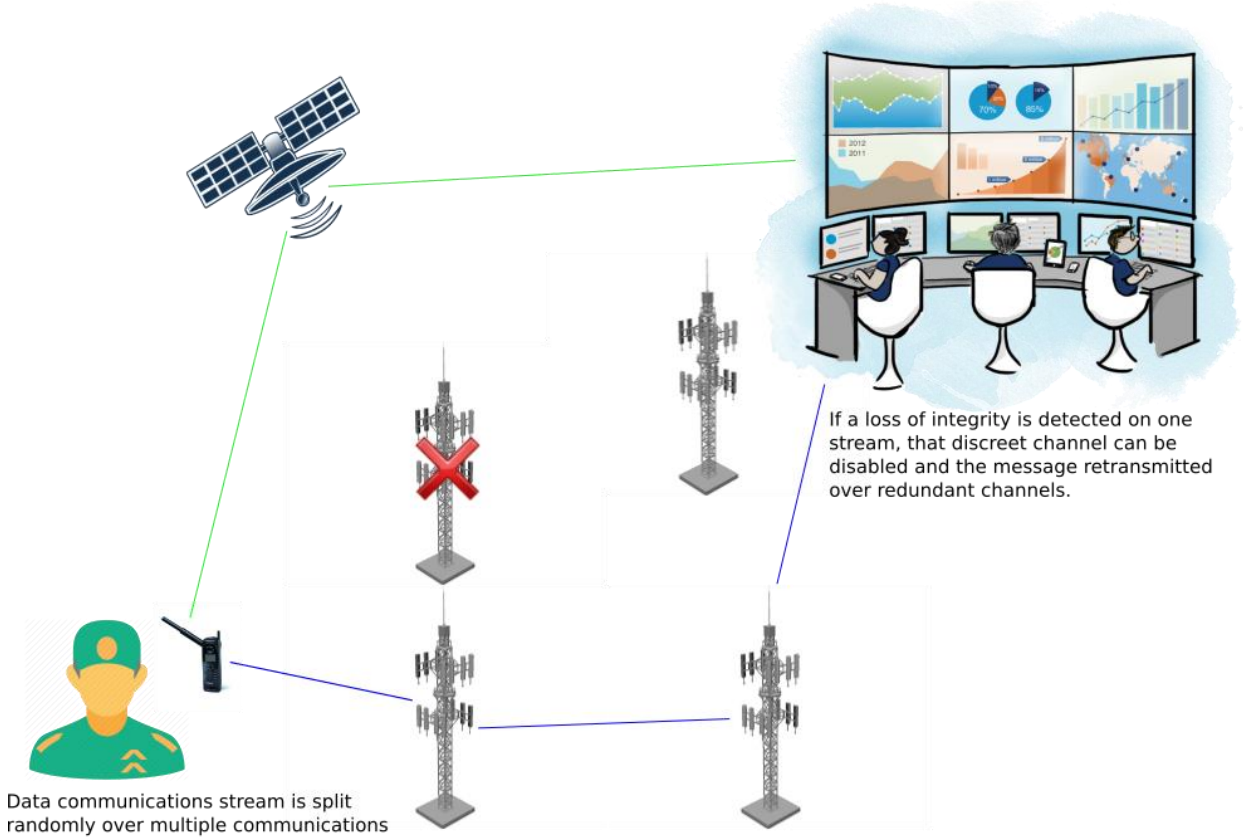
Medium stream splitting (MSS) involves splitting up a data transmission between multiple mediums.

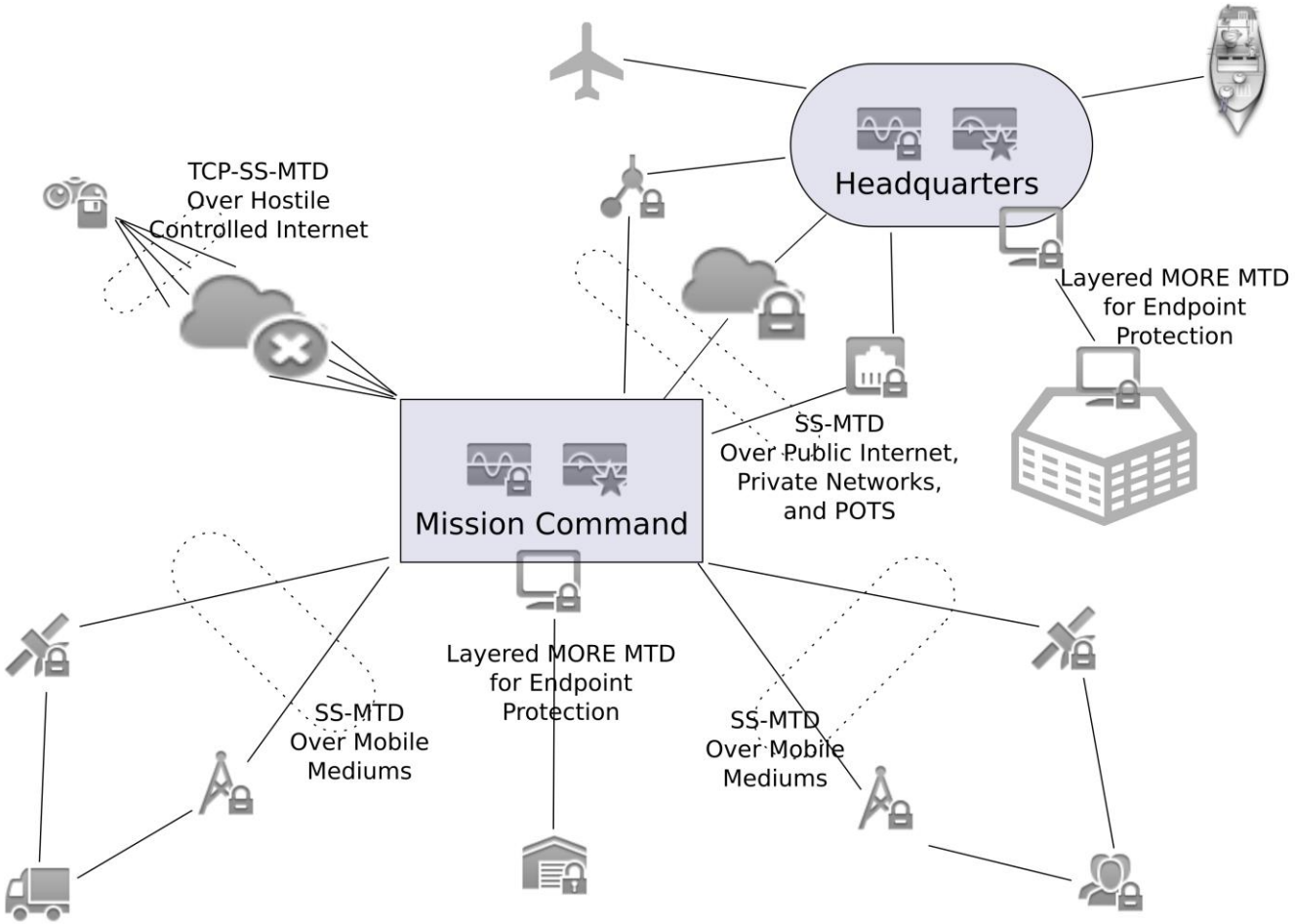
Mediums may include one or multiple physical network connections (e.g., cable and digital subscriber line [DSL]), radio, wireless, cellular, and public switched telephone network.




1, 4, 6, 7, 10, 11, 13, 15...
2, 3, 5, 8, 9, 12, 14...
Data is reassembled at the reciever. An error in one stream suggests compromise or transmission medium degredation. That channel can be eliminated and communication falls back to verifiable good channels.
Data communications stream is split randomly over multiple communications mediums by the sending device


Additional discreet paths, even over the same media type, allows for additional redundancy and add resilience in the event of a compromised or degraded channel.
Data communications stream is split randomly over multiple communications mediums by the sending device


If a loss of integrity is detected on one stream, that discreet channel can be disabled and the message retransmitted over redundant channels.
Data communications stream is split randomly over multiple communications mediums by the sending device


Headquarters
TCP-SS-MTD
Over Hostile
Controlled Internet
Layered MORE MTD
for Endpoint
Protection
SS-MTD
Over Public Internet,
Private Networks,
and POTS
Mission Command
Layered MORE MTD
for Endpoint
Protection
SS-MTD
Over Mobile
Mediums
SS-MTD
Over Mobile
Mediums

SS-MTD

Stream Splitting Moving Target Defense

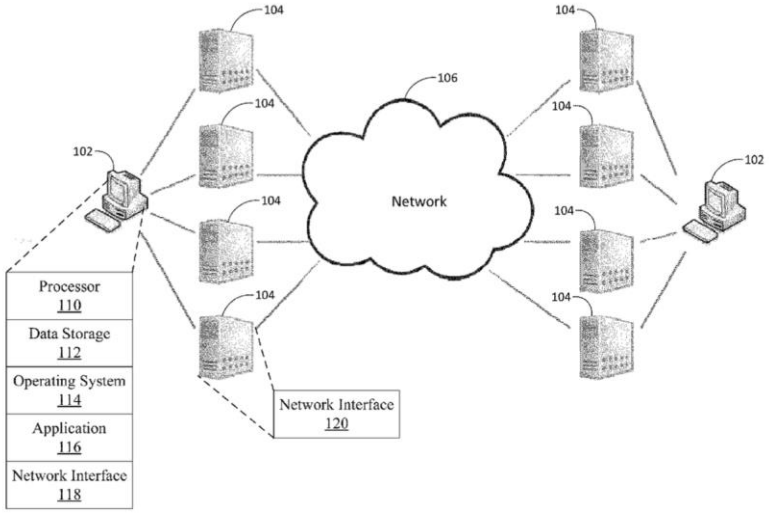
TRL:
2

IP Protection:
- Patent US 2018/0097764 A1

PROBLEM ADDRESSED
Critical lines of internet communication can be susceptible to the availability, confidentiality, and integrity of their internet service provider. Should the sole connection provided to a critical service go down, that service would become unavailable. Furthermore, should that provider act maliciously by participating in traffic interception and man-in-the-middle attacks, the privacy and integrity of the information would become compromised. These issues present themselves when a user relies on a singular connection to the internet.

TECHNOLOGY SOLUTION
Stream splitting moving target defense splits a stream of network packets among multiple network media such as fiber, cable, DSL, cellular, and packet radio. These split streams are forwarded to intermediate nodes across the internet to improve path diversity to anonymize the intended recipient and obfuscate possible points of interception. The use of multiple types of network media and internet paths also improves availability as the service is no longer subject to the uptime of a singular internet service provider.

DEPLOYMENT PATH
Tool is in conceptional phase and needs to be demoed more widely before adoption.



Initial Idea based on MORE-MTD — 2017

Prototype deployed in Africa to handle network resilience — 2019

Patent Granted — 2020