

GS-2300 Airborne C4ISR System

Integrated Tactical Command & Control System

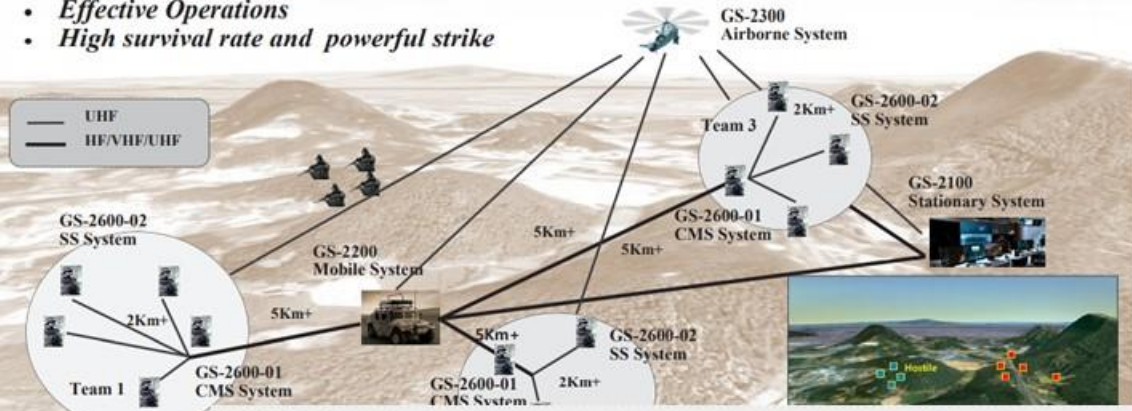
Compatible with Almost Aircrafts



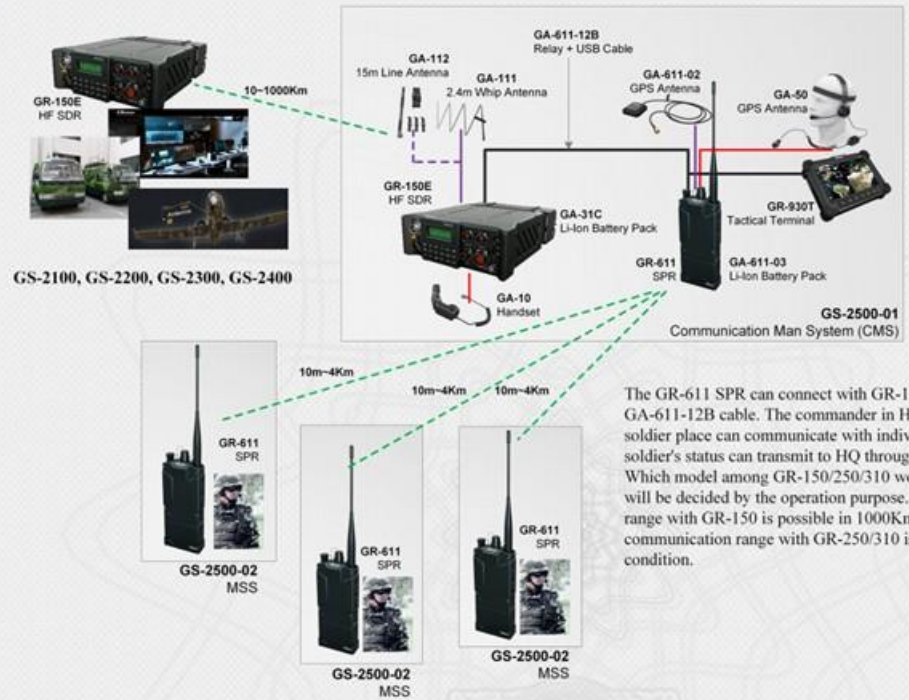
C4ISR Soldier System

GS-2500 Universal Soldier Information System

- Improves Situation Awareness
- Effective Operations
- High survival rate and powerful strike



GS-2500 Application Sample



The GR-611 SPR can connect with GR-150/250/310 through GA-611-12B cable. The commander in HQ which is far from soldier's place can communicate with individual soldiers. The soldier's status can transmit to HQ through GR-150/250/310. Which model among GR-150/250/310 would be connected will be decided by the operation purpose. The communication range with GR-150 is possible in 1000Km range, but the communication range with GR-250/310 is restricted by LOS condition.

북한 위협과 사이버작전 전망

2024. 1. 11. 교수 강동수

2024년 안보정세 키워드

✓ 북한 제8기 제9차 전원회의 (2023.12.)

- 핵무기 생산 지속과 2024년 정찰위성 3기 발사
- 현대전 특성에 맞게 무인장비들과 위력한 전자전 수단들 개발

✓ 북한궤 사이버위협 및 신기술 활용 사이버공격 증대 (2024년 전망, 국가안보전략연구원)

- 핵개발 자금 지원 목적의 암호화폐와 금융기관에 대한 사이버공격 및 랜섬웨어 범죄가 더욱 증대 될 것으로 예상되며 첨단기술을 탈취하기 위한 북한의 해킹도 지속될 것으로 전망
- 피싱 공격 · 딥페이크 · 탐지 회피 자동화 멀웨어 등 신종공격기법 확산

✓ 사이버 공격을 중심으로 하는 북한의 하이브리드 위협 (2024 안보정세 전망, KIDA)

- 2022년 북한이 사이버 공격을 통해 탈취한 암호화폐 액수는 전 세계 피해액의 절반 이상을 차지
- 국제사회는 북한이 사이버 공격을 통해 불법 획득한 자금을 핵·WMD 개발에 전용할 가능성 주목

※ 적의 미사일을 발사 준비단계에 서 무력화시키는 사이버 공격 작전능력이 강조

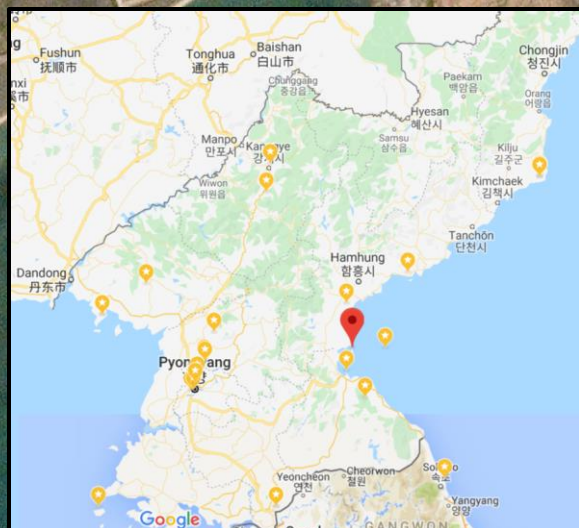
10:54 am Korea Standard Time
May 4, 2019

MISSILE LAUNCH HODO PENINSULA, DPRK

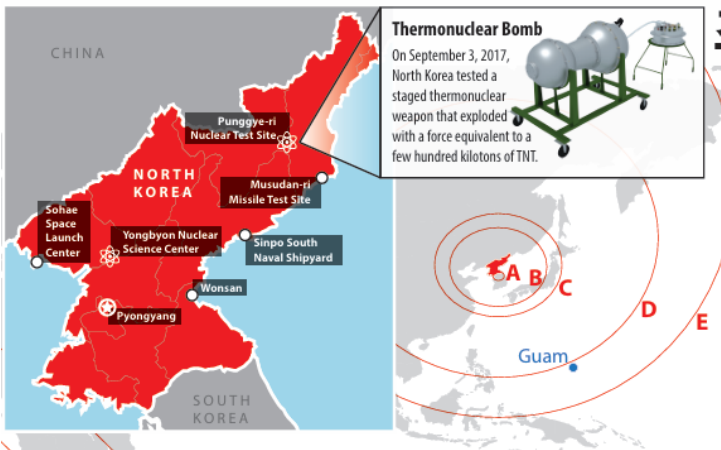
39.409561 N, 127.532835 E°

EXHAUST FROM THE LAUNCH

LAUNCH POINT



Middlebury Institute of
International Studies at Monterey
James Martin Center for Nonproliferation Studies



북한 7차 핵실험 ?

구분	정부	유관기관 및 전문가	종합 평가
1-3차	<ul style="list-style-type: none"> 폭발력: 0.8kt(1차), 3-4kt(2차), 6-7kt(3차) 	<ul style="list-style-type: none"> 폭발력: 1kt 미만(1차), 2-6kt(2차) 최대 40kt(3차, BER) 	<ul style="list-style-type: none"> 소형화/경량화 수준 미도달 (국방부 발표 기준)
4차 (2016.1.6.)	<ul style="list-style-type: none"> 리히터 규모: 4.8 폭발력: 6kt 	<ul style="list-style-type: none"> 리히터 규모: 4.8(KMA), 4.9(CEN C), 5.1(EMSC, USGS) 폭발력: 6.3kt(4.8, CTBTO) - 20.6kt(5.1, Murphy) 	<ul style="list-style-type: none"> CTBTO 산출 공식 적용시 최소 6.3kt에서 최대 12.6kt 까지 추정 가능 증폭핵분열탄 추정
5차 (2016.9.9.)	<ul style="list-style-type: none"> 리히터 규모 : 5.0 폭발력: 10kt 	<ul style="list-style-type: none"> 리히터 규모: 5.0(KMA), 5.0 (CENC), 5.2(EMSC), 5.3(USGS) 폭발력: 10kt(5.0, CTBTO) - 34.6kt(5.3, Murphy) 	<ul style="list-style-type: none"> 10-20kt 폭발력 추정 가능 (CTBTO 기준) 국제표준탄(15~20kt, 히로시마급) 수준 폭발력 표준화된 내폭형 핵탄두 실험 추정
6차 (2017.9.3.)	<ul style="list-style-type: none"> 리히터 규모 5.7 50kt 	<ul style="list-style-type: none"> 리히터 규모 6.3(미국) 100~300kt 	-

뉴스광장 1부

“KAMD 완성 위해 SM-3 도입 필요”...국방부 보고서 공개

입력 2017.09.13 (06:06) | 수정 2017.09.13 (07:13)



홈 > 정치 > 통일·외교·안보

"北 EMP공격하면 막기 어렵다" ... 文정부, 4년전 보고 받고 뭉개

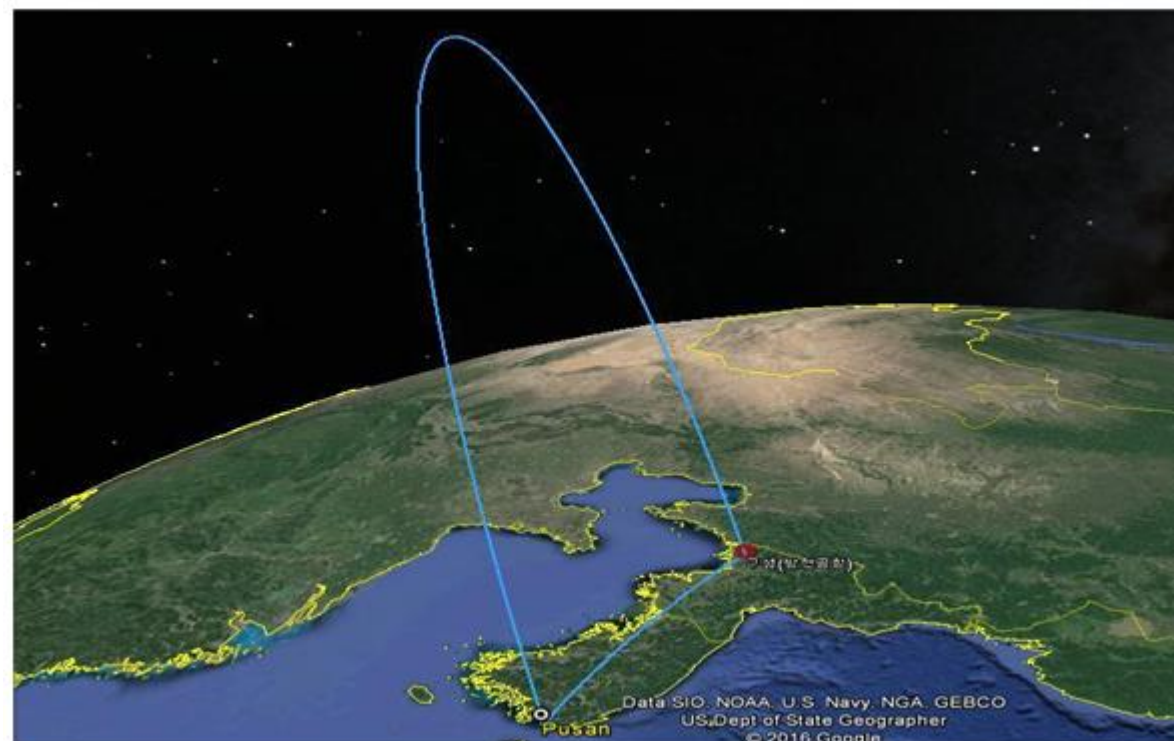
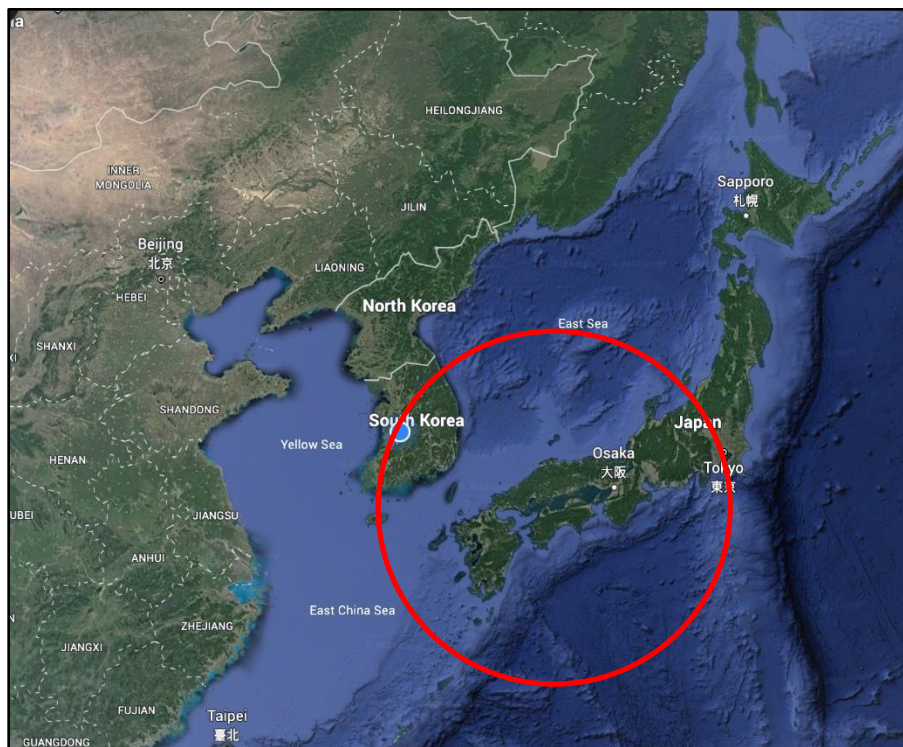
입력 2021.10.13 18:04:36 | 수정 2021.10.14 07:34:12



국방대 "고각 발사땀 요격 못해"
 '미국 SM-3 도입' 권고했지만
 정부 '중국 눈치'에 수용 안해



북한의 잠수함발사미사일(SLBM)인 북극성 1호 미사일이 지난 2017년 4월 15일 평양군사 행진에서 공개된 모습



<그림 30> 무수단 미사일 발사 시뮬레이션

$$Radius = 110\sqrt{HOB}$$

북한이 주변국의 영향을 최소화하기 위해 60-80km에서 핵탄두를 폭발시켜 EMP(Nuclear Electro Magnetic Pulse)를 발생시키는 수단으로 사용할 때는 반드시 요격해야 하는 문제이다.

출처: 강동수 외, KAMD 보강을 위한 해상탄도탄요격유도탄의 효용성에 관한 연구, 국방부, 2017.



See **ker**

MINUTEMAN III

ARMAMENT: NUCLEAR WARHEAD
THRUST: 202,600 LBS (91,170 KG)
LENGTH: 59.9 FT (18 METERS)
WEIGHT: 79,432 LBS (32,158 KG)
DIAMETER: 5.5 FT (1.67 METERS)
RANGE: 5,218 NAUTICAL MILES
SPEED: ~15,000 MPH (MACH 23)
CEILING: 700 MILES (1,120 KM)

BACKUP SELECT FOLDER.. ERASE (UNLOAD) ARCHIVE STORAGE

CYBERBORSTON DRONE DC

TRY STAR

W 189.1223 E 55.3117
N 49.7806 S 60.8429 SAT IN


LGM-30G ARSENAL: > 450

OPS DIAGNOSTIC DETAILS ANALYZE

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

SHIFT FINE TUNING OFFLINE MODE

6' TALL MAN



FAS.ORG

U.S. Nuclear Missiles Are Still Controlled
By Floppy Disks

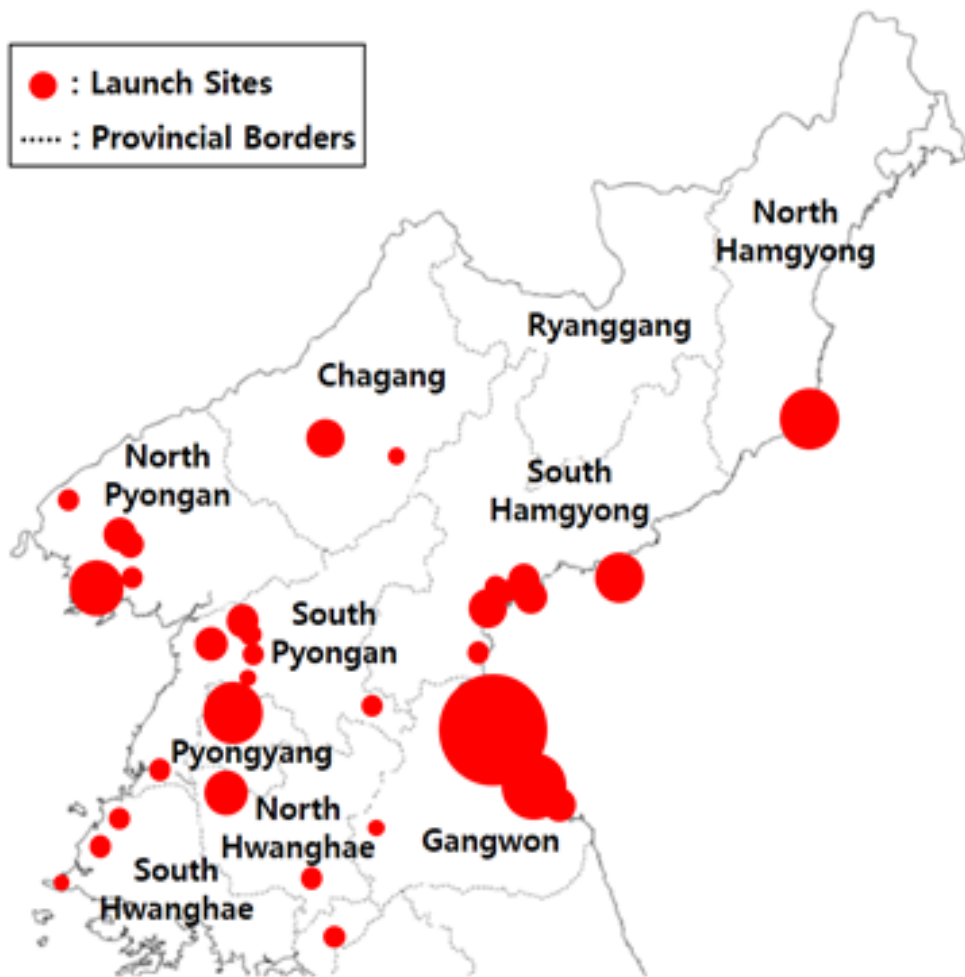


그림 5 탄도미사일 발사 지역
 Fig. 5 Ballistic Missile Launch Sites

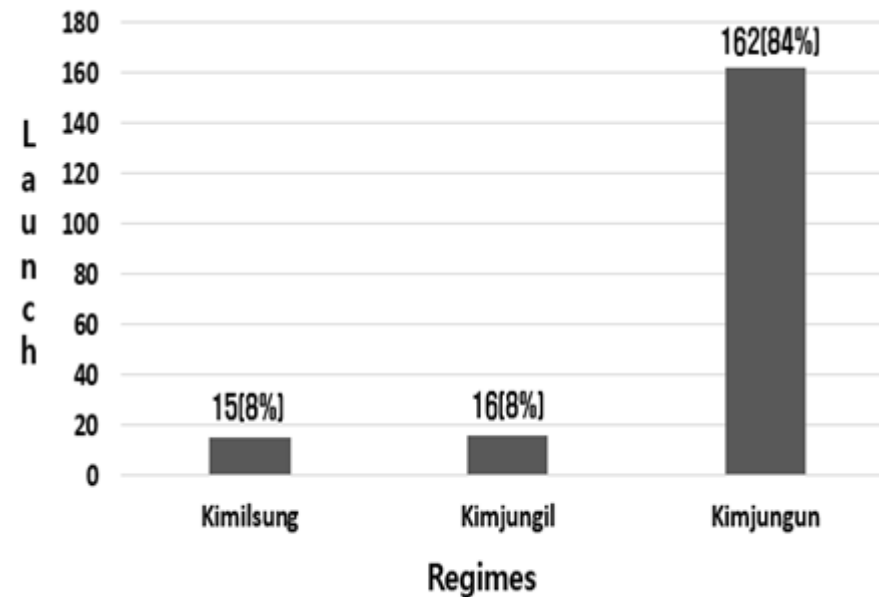


그림 3 정권별 탄도미사일 발사 횟수

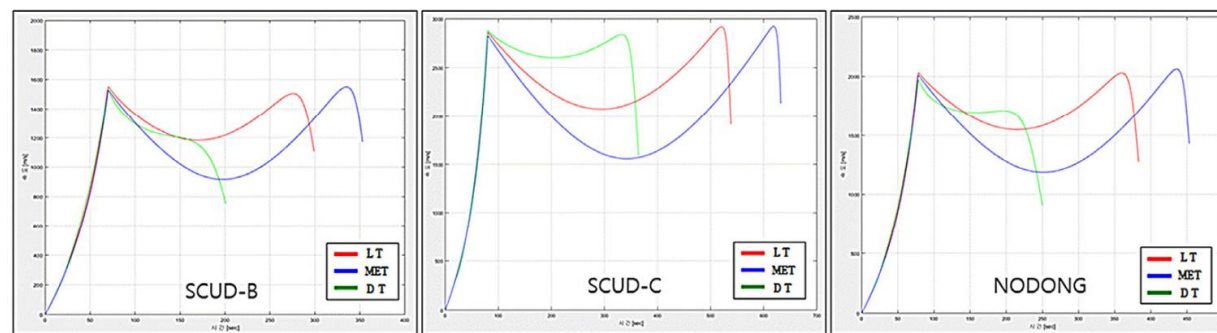


그림 5 시간에 따른 탄도미사일 속도 변화
 Fig. 5 The corresponding velocity change in ballistic missiles

오주호, 강동수, LSTM을 이용한 탄도미사일 사거리 예측, 2022.

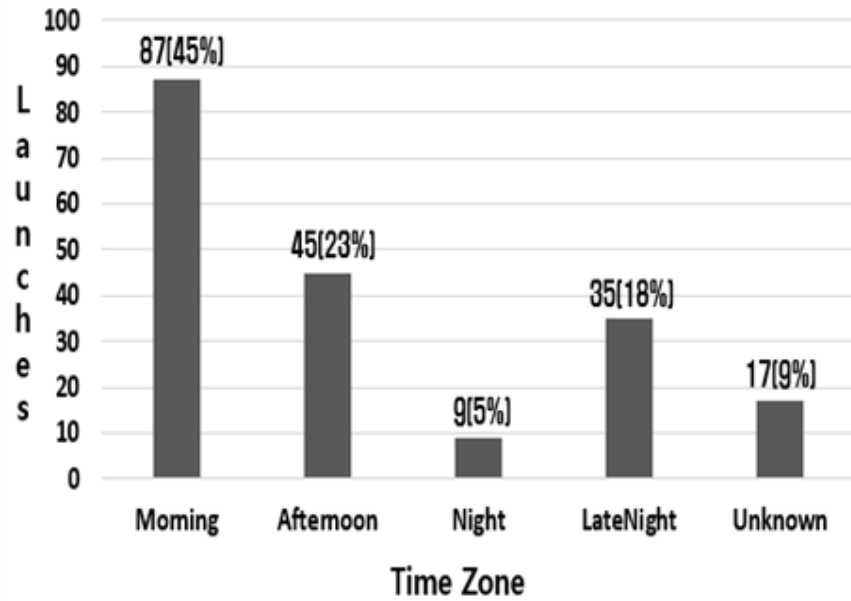


그림 7 시간대별 발사 횟수

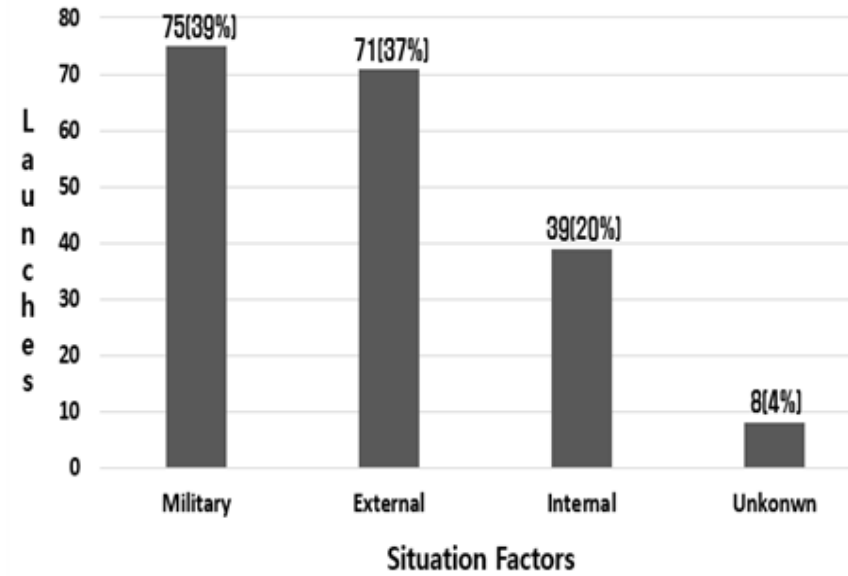
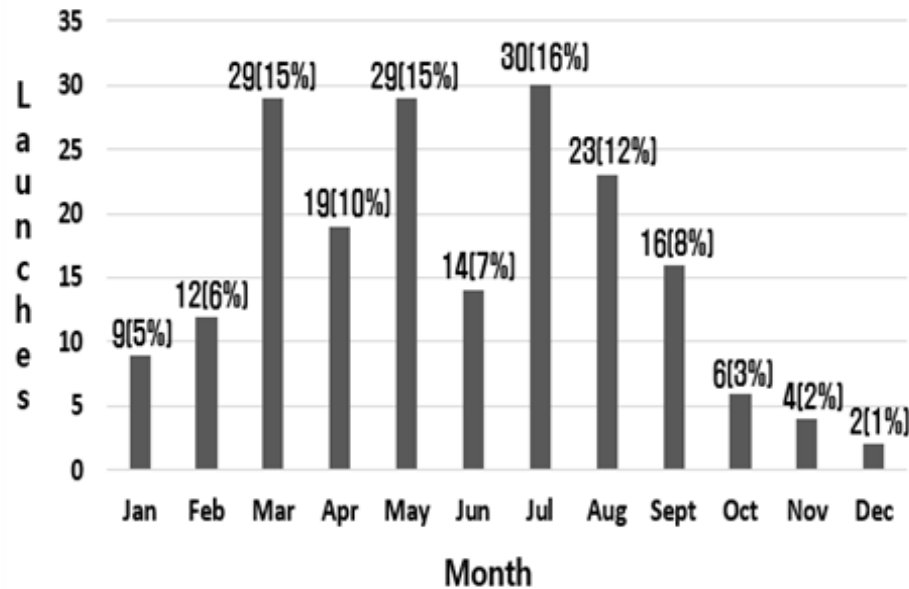


그림 8 탄도미사일 발사 관련 정세 요인

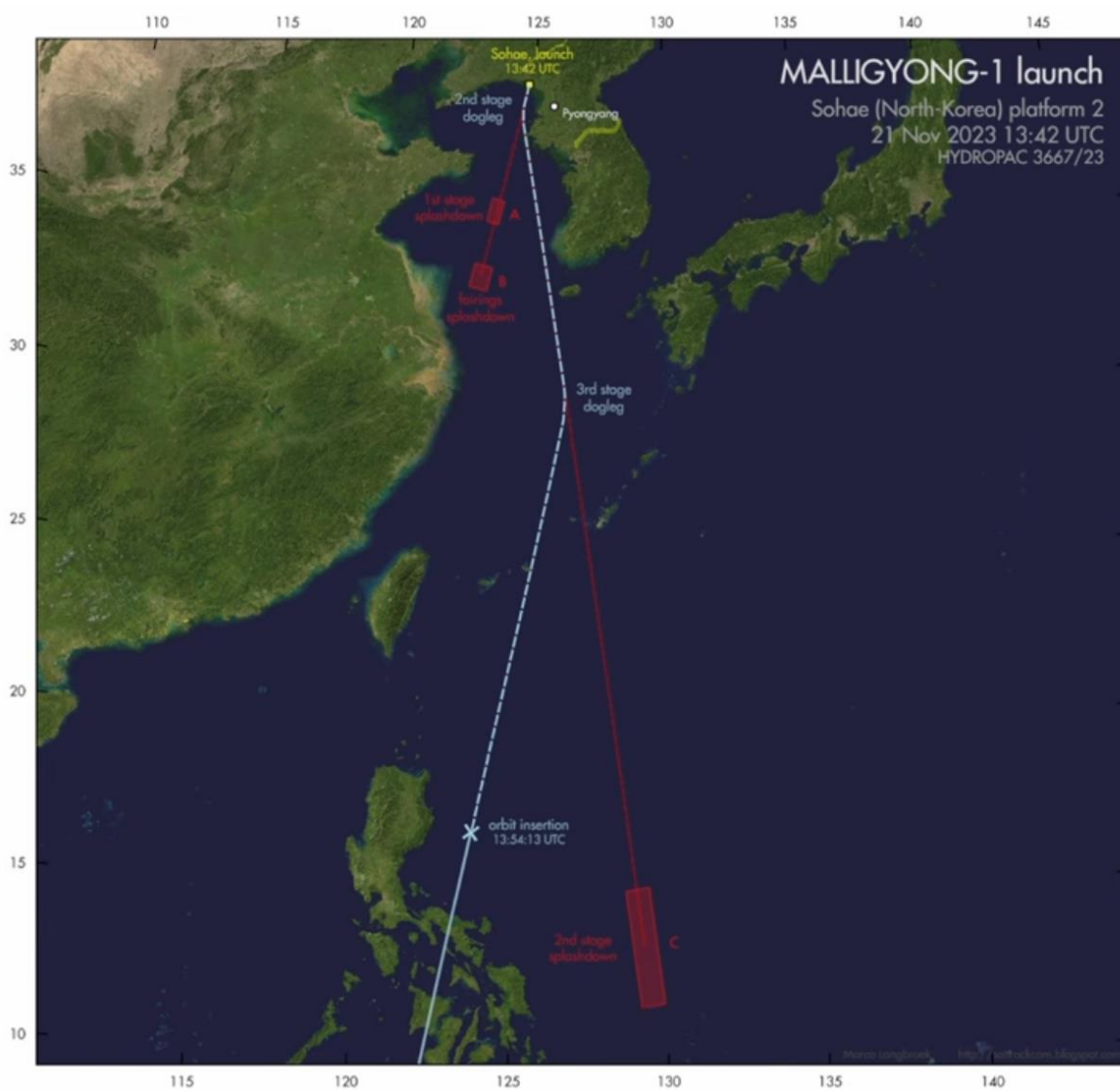


Launch Mission Execution Forecast	
Mission: Delta IV Heavy L-44	
Issued: 27 Aug 2020 / 1600L (2000Z)	
Valid: 29 Aug 2020 / DURING WINDOW	
Forecast Discussion: A pattern change will turn winds to the southwest through the weekend. This will bring an increased chance of afternoon and evening thunderstorms to the Spaceport each day as sea breeze interactions become more likely. For MST Roll Friday evening, scattered showers and thunderstorms capable of producing strong wind gusts are expected. These storms are expected to dissipate late in the evening, but lingering cloud cover from this activity will bring a small chance for a Thick Cloud Layer Rule violation during the launch window early Saturday morning. Offshore flow will strengthen further over the weekend as a frontal boundary moves into the southeastern US, resulting in a continued elevated chance of showers and storms, especially in the afternoon and early evening. This will maintain at least a small chance for a Thick Cloud Layer Rule violation in the event of a 24- or 48-hour delay.	
Launch Day	Probability of Violating Weather Constraints 20% Primary Concerns: Thick Cloud Layer Rule Weather Conditions Weather/Visibility: None / 7 mi. Type: None Temp/Humidity: 80°F / 92% Ground Winds (300'): 230° @ 8 - 13 knots Clouds: Scattered 18,000 20,000 Solar Activity: Low
	Probability of Violating Weather Constraints 30% Primary Concerns: Thick Cloud Layer Rule Weather Conditions Weather/Visibility: None / 7 mi. Type: Altostratus Temp/Humidity: 79°F / 93% Ground Winds (300'): 240° @ 11 - 16 knots Clouds: Broken 15,000 19,000 Solar Activity: Low
	Probability of Violating Weather Constraints 20% Primary Concerns: Thick Cloud Layer Rule Weather Conditions Weather/Visibility: None / 7 mi. Type: Altostratus Temp/Humidity: 78°F / 94% Ground Winds (300'): 250° @ 8 - 13 knots Clouds: Scattered 15,000 19,000 Solar Activity: Low
<small>Note: The Probability of Violator (POV) is the chance that a Launching Launch Control Criteria (LCCO) or launch user constraints (surface winds, precipitation, and temperatures, etc.) will be violated during the launch window. It does not take into account upper-level wind shear and solar activity.</small> Next Forecast Will Be Issued: 28 Aug 2020	



그림 9 북한 기상관측 지점

Fig. 9 Meteorological Observatory of North Korea



- Malligyong-1 #3, Chollima-1
- NORAD ID: 58400
- Observation: 468.738 MHz,
- Semi major axis: 6880 km
- RCS: Unknown
- Launch date: November 21, 2023
- Source: North Korea (NKOR)

```
[ ] 1 audio_path = '/content/sample_data/satnogs_8603853_2023-11-28T20-57-47.ogg'
```

```
1 from IPython.display import Audio
2 Audio(audio_path)
```

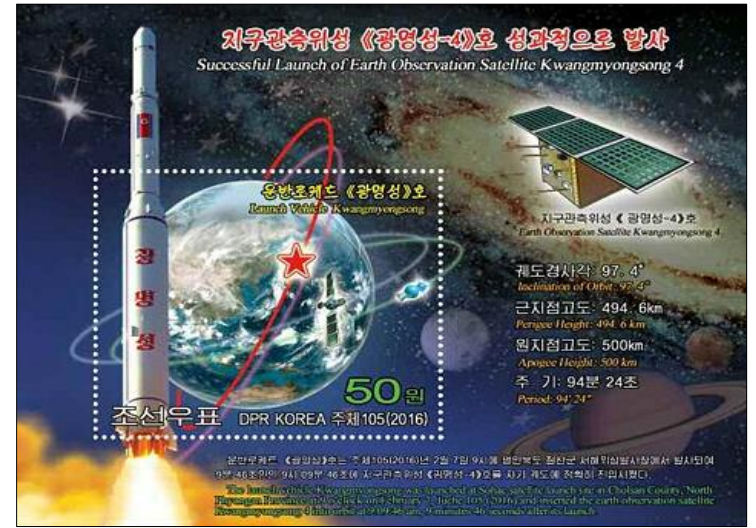
0:06 / 7:17

구 분		백두산 로켓 대포동 1호	은하 1호 대포동 2호	은하2호 대포동 2호	은하 3호 (1차)	은하 3호 (2차)	은하 3호 (개량)
연료	1단	액체	액체	액체	액체	노동엔진	노동엔진
	2단	액체	액체	액체	액체	스커드엔진	스커드엔진
	3단	-	고체	고체	미상	미상	미상
크기	1단 직경	-	2.2m	2.2m	2.2m	2.4m	-
	1단 길이	-	17m	17m	-	-	-
	2단 직경	-	1.5m	1.5m	-	-	-
	2단 길이	-	14m	14m	-	-	-
총길이		27m	32m	32m	35.8m	30m	미상
총중량		21톤	60톤	60톤	79톤	91톤	미상
사거리		2,200km	6,000km	6,000km	10,000km	12,000km	미상
탄두 중량		1톤	1톤	1톤	1톤	2톤	미상
발사장소		무수단	무수단	무수단	동창리	동창리	동창리
시험발사일		1998.08.31.	2006.07.04.	2009.04.05.	2012.04.13.	2012.12.12.	2016.02.07.

- 우주발사체 능력: 러시아('57), 미국('58), 유럽('65), 중국('70), 일본('70), 영국('71), 인도('80), 이스라엘('88), 이란('09), 북한('12)
- 다탄두 발사 능력 : 미국, 러시아, 중국, 영국, 프랑스, 파키스탄, 인도

출처: 강동수, 북한 우주개발 기술 현황 조사, 2022.

발사체	위성	NORAD ID	발사일	비행종료	현상태	발사장소
백두산 로켓 대포동 1호	광명성1호	진입실패	1998.08.31.	1단 95초 2단 144초 3단 27초	-	동해발사장 (무수단리)
은하 1호(추정) 대포동 2호	-	진입실패	2006.07.04.	-	-	
은하 2호 대포동 3호	광명성2호	진입실패	2009.04.05.	-	-	
은하 3호	광명성3호	진입실패	2012.04.13.	135초	-	서해발사장 (동창리)
은하 3호	광명서3-2호 KMS 3-2	39026	2012.12.12.	-	작동중지	
UNHA 3 R/B	-	39027	2012.12.12	-	파편관측	
UNHA 3 DEB	-	39028	2012.12.12	2018.08.10.	-	
UNHA 3 DEB	-	39029	2012.12.12	2021.02.16.	-	
은하 3호 (개량)	광명서4호 KMS 4	41332	2016.02.02.	-	작동중	
UNHA 3 R/B	-	41333	2016.02.02.	-	파편관측	



- 소련 1957.10.
- 미국 1958.2.
- 프랑스 1965
- 일본 1965
- 중국 1970
- 영국 1971
- 인도 1980
- 북한 2012

출처: 강동수, 북한 우주개발 기술 현황 조사, 2022.



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)



DESCRIPTION 2018. 9. 6.

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	Hair: Black
Eyes: Brown	Sex: Male
Race: Asian	Languages: English, Korean



- Sony Pictures (2014)
- WannaCry 2.0 ransomware attack (2017)
- Cybertheft from the central bank of Bangladesh (2016)

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT **COPY**

for the
Central District of California

United States of America
v.
PARK JIN HYOK, also known as ("aka")
"Jin Hyok Park," aka "Pak Jin Hek,"
Defendant.

Case No. **18-1479**

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	Offense Description
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1349	Conspiracy to Commit Wire Fraud

This criminal complaint is based on these facts:
Please see attached affidavit.
BE Continued on the attached sheet.

Complainant's signature
Nathan P. Shields, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.
Date: 06-08-18
City and state: Los Angeles, California

Judge's signature
ROZELLA A. OLIVER
Printed name and title
Hon. Rozella A. Oliver, U.S. Magistrate Judge
Printed name and title

REC- Detention

러시아군 장교 6명 해킹작전 혐의로 미국서 기소

YURIY SERGEYEVICH ANDRIENKO
(Юрий Сергеевич Андрияшко)



SERGEY VLADIMIROVICH DETISTOV
(Сергей Владимирович Детистов)



PAVEL VALERYEVICH FROLOV
(Павел Валерьевич Фролов)



ANATOLIY SERGEYEVICH KOVALEV
(Анатолий Сергеевич Ковалев)



ARTEM VALERYEVICH OCHCHENKO
(Артем Валерьевич Очченко)



PETR NIKOLAYEVICH PLISKIN
(Петр Николаевич Плискин)



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, October 19, 2020

Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace

PyeongChang Winter Olympics Hosts, Participants, Partners, and Attendees:

December 2017 through February 2018 spearphishing campaigns and malicious mobile applications targeting South Korean citizens and officials, Olympic athletes, partners, and visitors, and International Olympic Committee (IOC) officials;

Pyongyang Blockchain and Cryptocurrency Conference



Our Success

The first Pyongyang Blockchain and Cryptocurrency Conference on April 2019 was a success where international experts in the Blockchain and Crypto industry gathered in Pyongyang to share their knowledge and vision, established long lasting connections, discussed business opportunities and signed contracts in the field of Information



Pyongyang Blockchain and Cryptocurrency Conference - 18th to 25th April 2019





Inside Marine Chain, The North Korean Scam ICO

 By Mark Hunter

1 YEAR AGO



← **MarineChain**
0 트윗



팔로우

MarineChain
@MarineChain

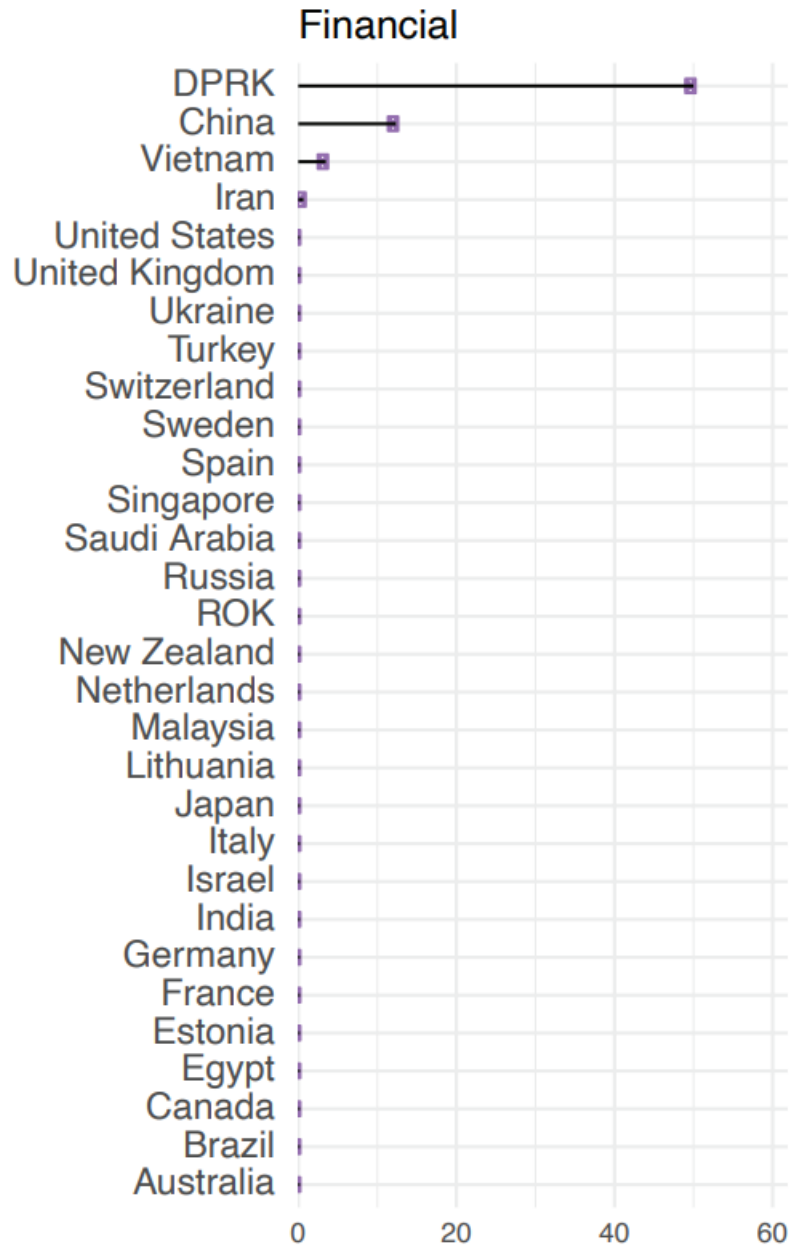
MarineChain Platform is the next generation of the global vessel market which is possible due to the blockchain.

📍 Hong Kong 🌐 marine-chain.io 📅 가입일: 2017년 11월

2 팔로우 중 6 팔로워

트윗 트윗 및 답글 미디어 마음에 들어요

National Cyber Power Score





REWARD

up to
\$5,000,000 USD

For information leading to the arrest and/or conviction of



WANTED FOR BANK FRAUD, MONEY LAUNDERING, AND SANCTIONS
EVASION

SIM HYON-SOP


+1-520-442-0703


Type	ID#	Country	Issue Date	Expire Date
Passport	109484100	Korea, North		24 Dec 2024
Secondary sanctions risk:	North Korea Sanctions Regulations, sections 510.201 and 510.210			
Transactions Prohibited For	North Korea Sanctions Regulations section 510.214			
Persons Owned or Controlled By U.S. Financial Institutions:				
Gender	Male			
Digital Currency Address - ETH	0x4f47bc496083c727c5fbc3ce9cdf2b0f6496270c			
Digital Currency Address - ARB	0x4f47bc496083c727c5fbc3ce9cdf2b0f6496270c			
Digital Currency Address - BSC	0x4f47bc496083c727c5fbc3ce9cdf2b0f6496270c			

Home » Ratings » Ratings - All

CODECHEF RATINGS (ALL)

[Tweet](#) [Like](#) [Share](#) 30 people like this. [Sign Up](#) to see what your friends like

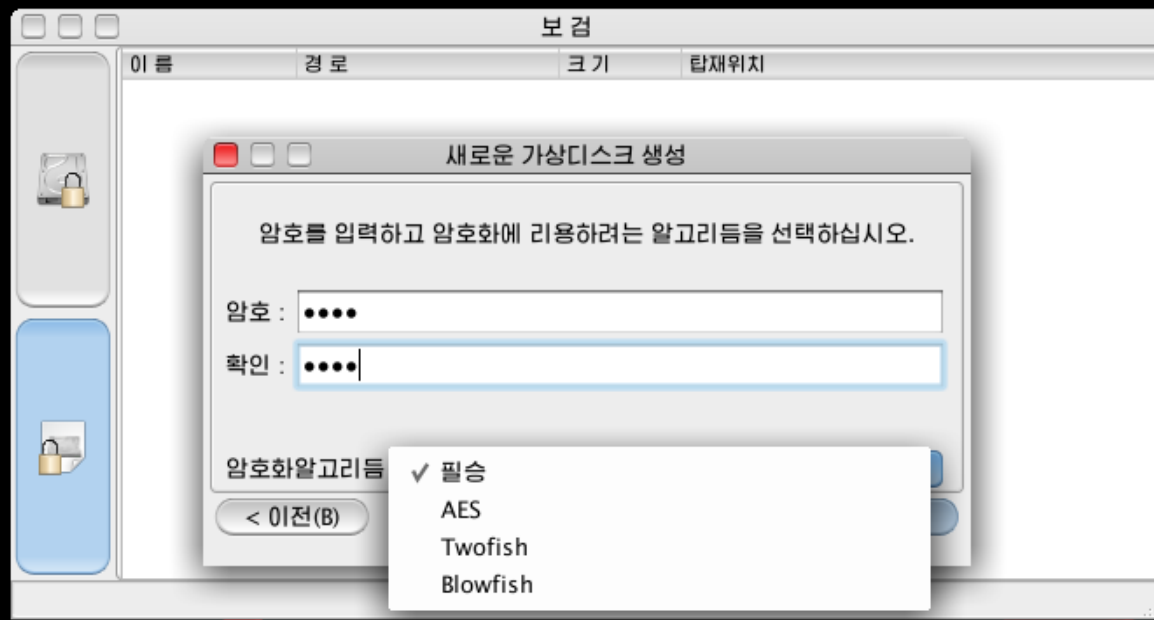
Calculated till DEC20B

Type to search & press enter Country

# GLOBAL(COUNTRY)	USER NAME
1 (1)	7★ gennady.korotkev... Saint Petersburg National Research University of Information Technologies,
2 (1)	7★ ACRush PonyAI
3 (1)	7★ ms4 Kim Il-sung University
3 (1)	7★ kut_hgs1997 Kim Chaek University of Technology
5 (3)	7★ kutengine Kim Chaek University of Technology



김책공대
김일성대학



- ✓ P I l s u n g
- ✓ AES(Advanced Encryption Standard): NIST(Rijndael), 2001.
- ✓ Twofish(1998): 128, 192, 256bit
- ✓ Blowfish(1993): 32~448bit



Known Threat Actors

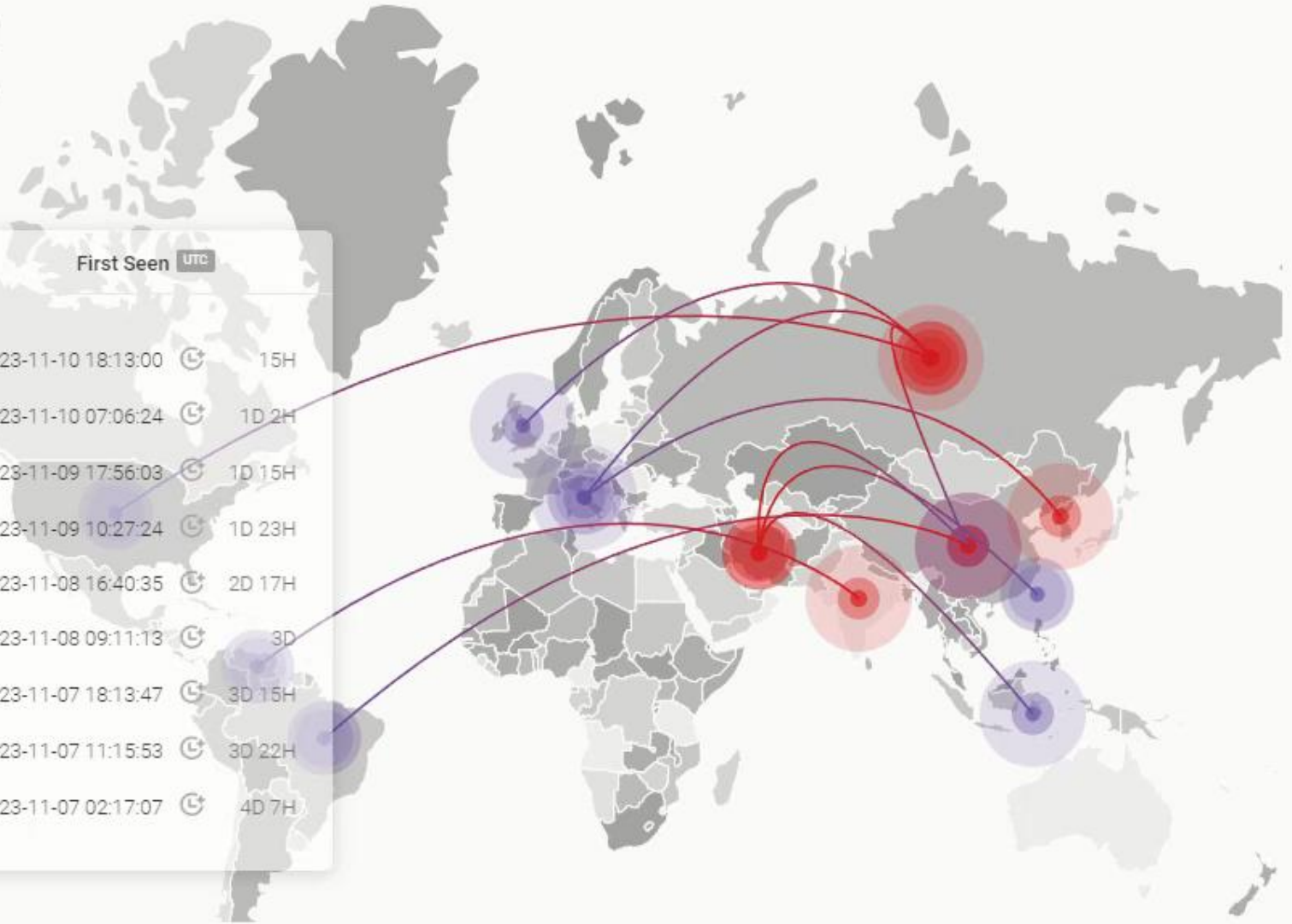
Total Threat Actors

* A:

🕒 2023-11-11 10:30:09 UTC

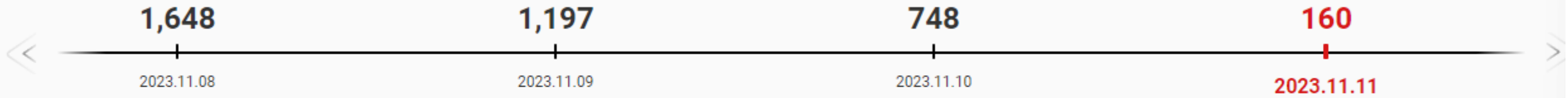
🕒 2023-11-11 19:30:09 local

Threat Actor	Targeted Countries	First Seen UTC
Gamared...	→	2023-11-10 18:13:00 🕒 15H
Salty Spider	→	2023-11-10 07:06:24 🕒 1D 2H
MuddyWa...	→	2023-11-09 17:56:03 🕒 1D 15H
Carbanak	→	2023-11-09 10:27:24 🕒 1D 23H
APT39	→	2023-11-08 16:40:35 🕒 2D 17H
Group123	→	2023-11-08 09:11:13 🕒 3D
Red Apollo	→	2023-11-07 18:13:47 🕒 3D 15H
SideWinder	→	2023-11-07 11:15:53 🕒 3D 22H
Operation ...	→	2023-11-07 02:17:07 🕒 4D 7H





































Recent Attack Activity Statistics

Number Of Campaigns



Threat Actors Top. 5

Threat Actor	Associated Campaigns	Targeted Countries Top. 3	Targeted Industries Top. 3
 Emote...	25	  	  
 DarkH...	12	  	 
 Lazaru...	7	  	  
 APT28	6	  	  
 Gorgo...	6	  	  

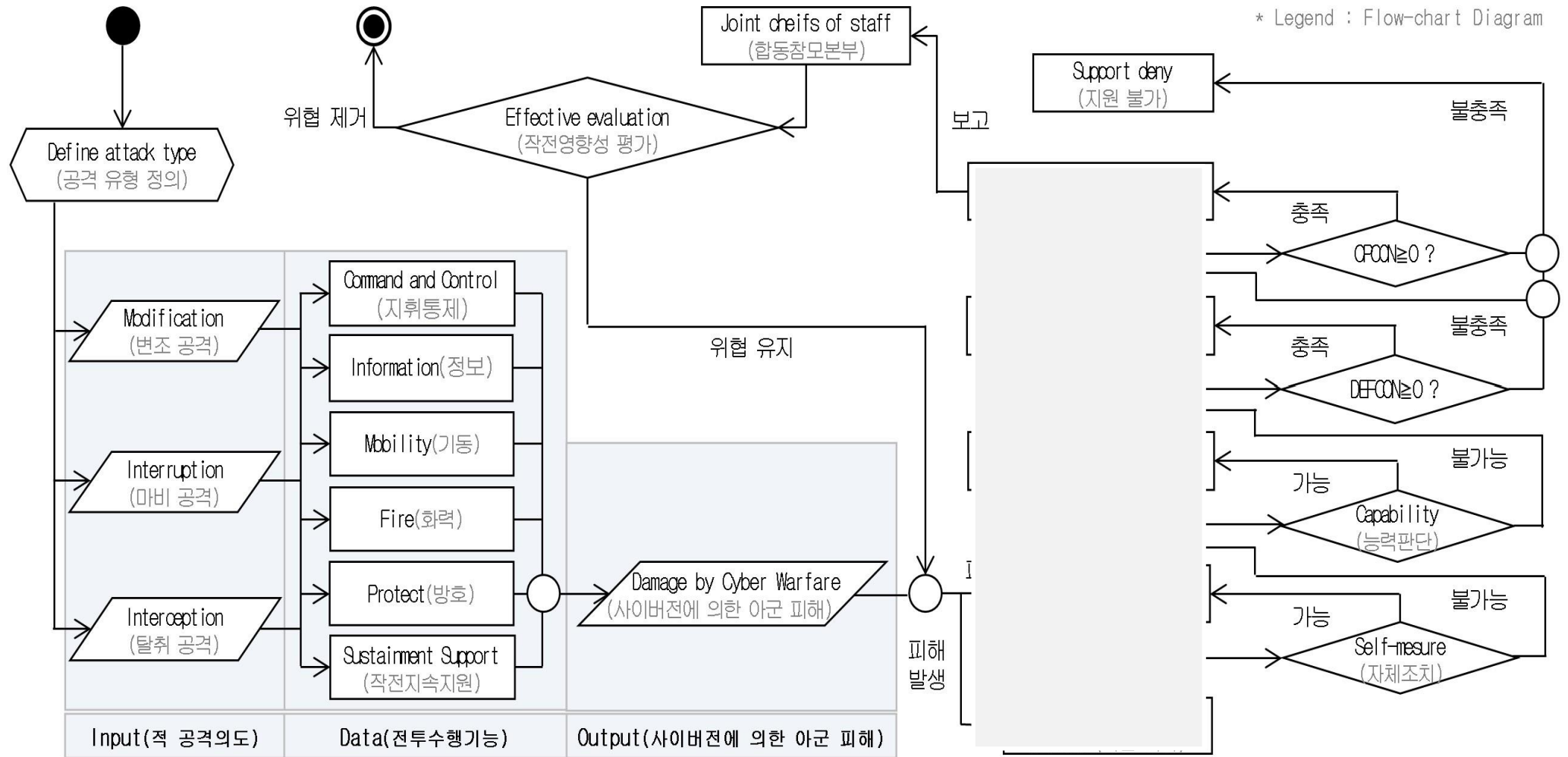
사이버 작전의 공격유형과 피해

✓ 정보보안의 3대 목표

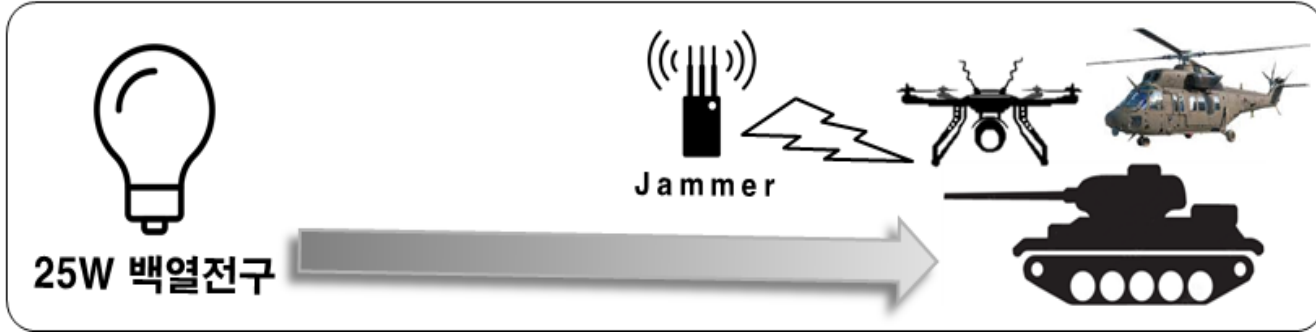
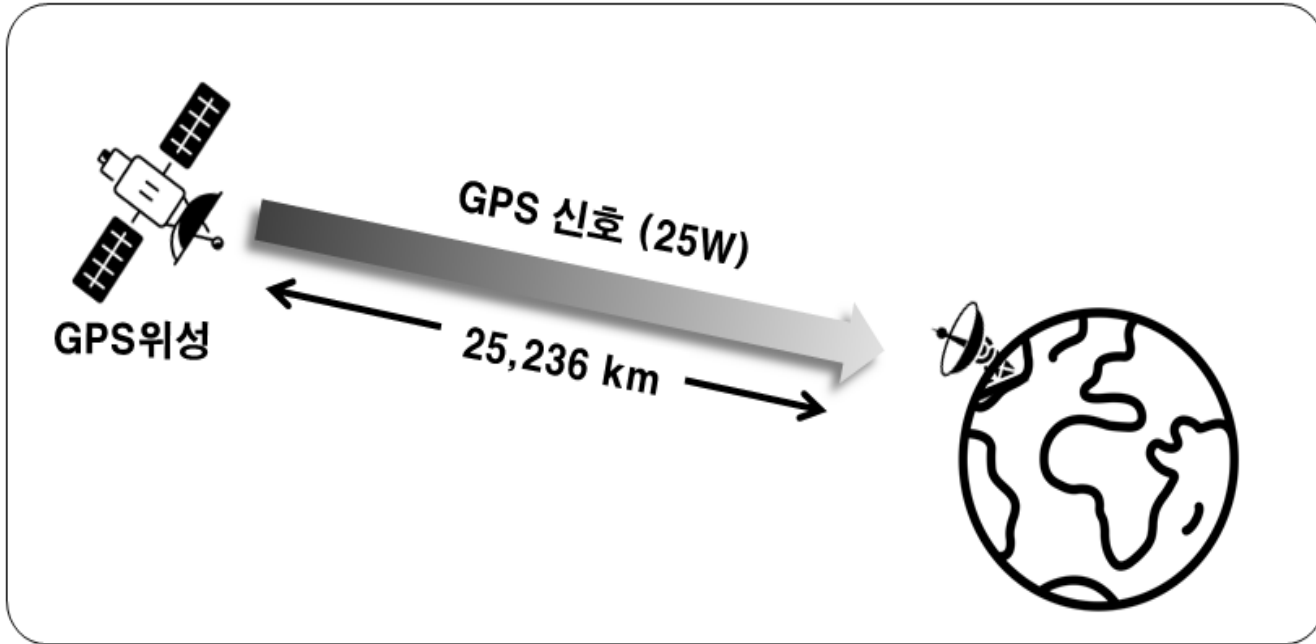
- 기밀성(Confidentiality) ← 변조(Modification)
- 무결성(Integrity) ← 탈취(Interception)
- 가용성(Availability) ← 마비(Interruption)

구분	변조(Modification)	마비(Interruption)	탈취(Interception)
정의	비인가자들의 불법적인 접근과 데이터의 변경 등 무결성 에 대한 공격	시스템의 일부 파괴 또는 사용불능 등 가용성 에 대한 공격	비인가자의 불법적인 시스템 사용과 정보획득 등 기밀성 에 대한 공격
공격 유형	SW공급망 공격 등	DDoS, 랜섬웨어 등	권한상승 등
공격 기법	웹 변조, 루트킷, XSS, SQL Injection, CSRF 등	랜섬웨어, 봇넷 C&C, Slowloris, Flooding, 버퍼오버플로우 등	백도어, MITM, 스니핑, 패스워드 크래킹 등
대응조치	<ul style="list-style-type: none"> ◦ 원본 파일의 해시값과 변조 추정 파일의 해시값 비교 ◦ 셸 감염여부 확인 후 삭제조치 ◦ 방화벽을 통한 접근 제한정책 적용, 시스템 재설치 	<ul style="list-style-type: none"> ◦ KISA 사이버대피소 등 DDoS 방어서비스 적용 ◦ 보안장비를 통한 IP 접근 차단 ◦ 악성코드 탐지를 위한 백신 최신화 운용 	<ul style="list-style-type: none"> ◦ 운영체제 최신 보안 패치 ◦ 방화벽을 통해 공격에 활용된 Port 차단정책 적용 ◦ 특정 포트 서비스로 실행중인 파일 확인 및 삭제
정보보호체계	<ul style="list-style-type: none"> ◦ 웹변조탐지 (홈페이지 위·변조) 	<ul style="list-style-type: none"> ◦ NTAS (네트워크 트래픽 분석) 	<ul style="list-style-type: none"> ◦ SIEM(통합로그관리)
	<ul style="list-style-type: none"> ◦ IPS(실시간 침해 탐지/차단), UTM(IP 및 서비스 통제, 방화벽) 		

사이버 작전 수행 알고리즘



GPS 전파교란 원리와 수신 세기



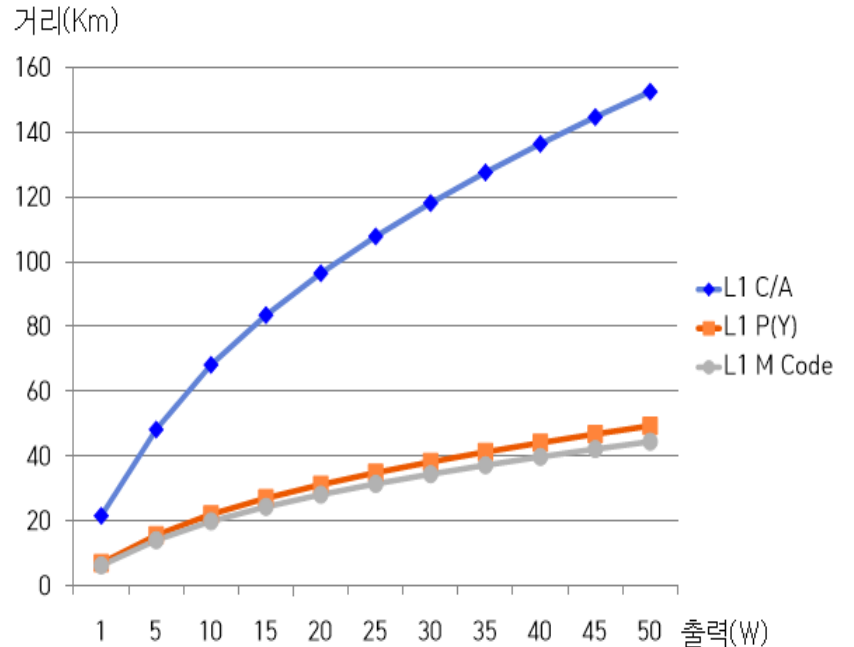
✓ 지상에서 받는 GPS 신호의 수신 세기

- 위성방출전력값 + 대기/편광손실 + 자유공간 경로 손실

$$= 24.10\text{dBW} - 0.5\text{dB} - 184.43\text{dB} = -160.83\text{dBW}$$

$$= -130.83\text{dBm}$$

$$d=25,236\text{km}, f=1,575.42\text{MHz}, c=3 \times 10^8\text{m/s}$$



GPS 스푸핑(Spoofing) 공격으로 미국 RQ-170 무인기 나포



<그림 6> 이란의 드론 모습

출처: Chris Wozny, RQ-170 Drone Hacking

이란 북부 카시마르(Kashmar) 상공에서 비행중이던 무인기 발견 → 위성/지상에서 무인기로 향하는 모든 신호 재밍 → 기만 GPS 송신(spoofing) → RQ-170 칸타하르 기지착륙

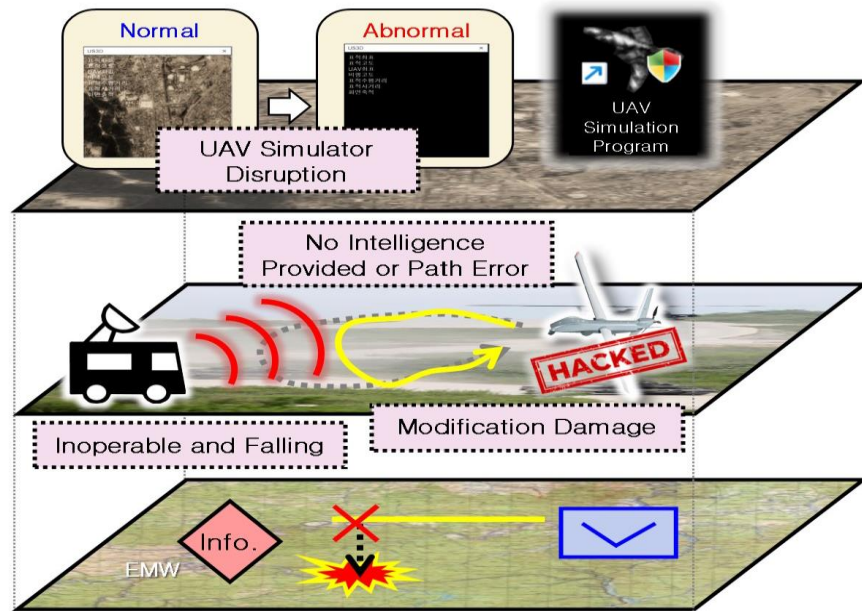
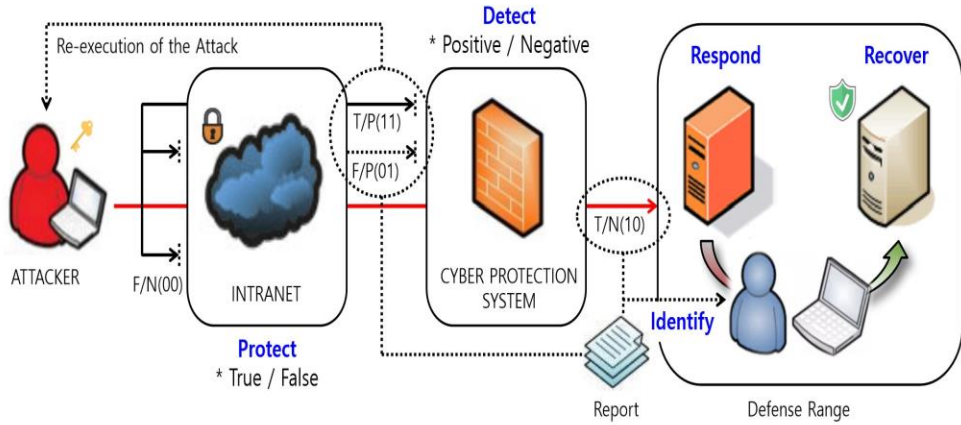
구분	내용	구분	내용
임무	정보, 감시, 표적 획득, 정찰 및 전자전	높이	1.21m ~ 1.82m
승무원	없음	전력용량	9,275lbs
도입년도	2007년	Type	GE turbofan engine
날개 길이	14m ~ 27.43m	엔진 수	1개
Service Ceiling ¹¹⁾ (실용상승한도)	50,000피트(15,240m)	제조사	Skunk Works (a division of Lockheed Martin Corporation)

GPS 피해 유형

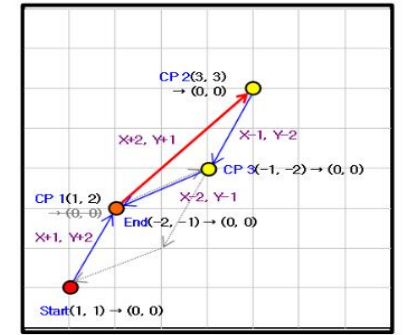
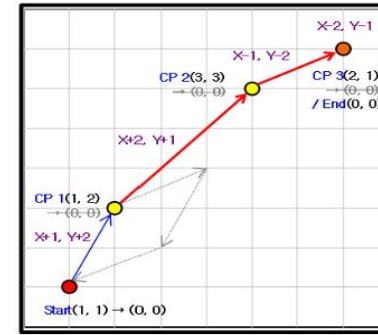
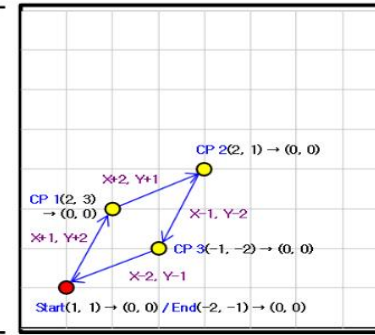
- ✓ 실제 GPS 교란상황 시, 재밍 신호는 GPS 위성신호 전력(-130dBm)대비 약 천만배 큰 신호인 약 -70dBm 신호가 유입
- ✓ 북한으로부터 GPS 전파교란 현황

구분	1차	2차	3차	4차
발생일시	'10.8.23~26(4일)	'11.3.4~14(11일)	'12.4.28~5.13(16일)	'16.3.31~4.5(6일)
발신지	개성	개성, 금강산	개성	해주, 연안, 개성, 평강, 금강산
신호유입	수도권 서북부	수도권 서북부 및 강원	수도권 서북부	인천서부, 중서부, 중부, 강원도 일부
신호세기	-70dBm~-60dBm	-60dBm	-80dBm~-60dBm	-79dBm~-67dBm

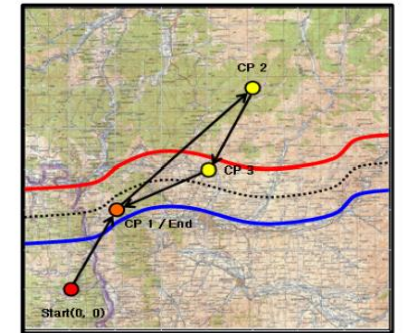
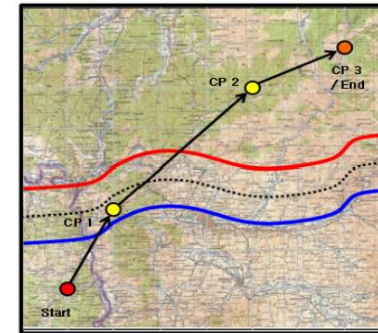
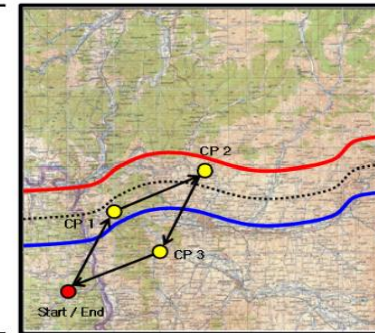
- ✓ 김포공항 인근 GPS 혼신 사례 (2022.1.24~2022.1.27) 김포공항 북서쪽 약 14km 지점에서 민항기 GPS 혼신 신고



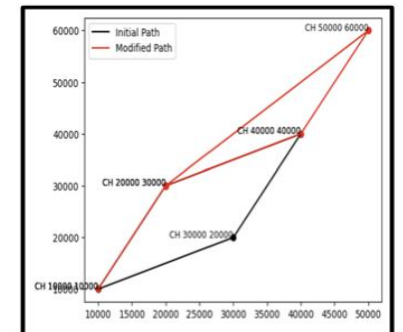
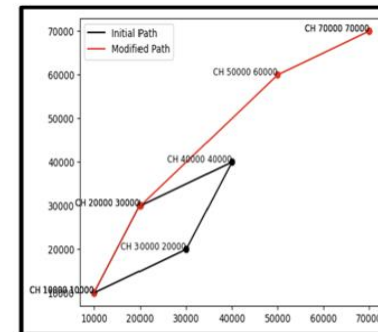
Design



Modeling



Realization



감사합니다.

국방대학교 교수 강동수

greatkoko@kndu.ac.kr

