





역 HYPO

해군 암호학의 과거, 현재 및 미래 축하

미국 함대 사이버 사령부 / 미국 10 대 함대 – 전략 계획
2020-2025





사령관의 서문

최근에 10 주년을 맞이했습니다. 지난 10 년 동안 Fleet Cyber Command / TENTH Fleet, 해군 및 전 세계에서 많은 변화가 있었습니다.

이 사령부는 전 세계에 걸쳐 55 개의 사령부와 40 개의 사이버 미션 부대로 구성된 14,000 명 이상의 현역 및 예비 선원과 민간인으로 구성된 작전 부대로 성장했습니다. 우리는 해군의 정보 네트워크 운영, 공격 및 방어 사이버 공간 운영, 우주 및 정보 운영, 신호 인텔리전스를 담당합니다. 우리는 미국 사이버 사령부, 국가 안보국의 해군 구성 요소로 활동하고 있으며 최근에는 해군 우주 사령부, 미국 우주 사령부의 구성 요소 및 미국의 새로운 우주 부대로 지정되었습니다.

Vital C2 네트워크는 함대를 연결하여 분산 해양 작전을 가능하게 합니다. 실시간 경고 및 표적 생성은 TACSIM을 뒷받침하고 통합 화재를 강화합니다. 사실상 DMO의 모든 측면은 정보 전쟁의 성공 여부에 달려 있습니다. 우주의 높은 지대에서 사이버 공간의 "모든 지대"를 통해 우리는 오늘날 가장 빠른 전투를 주도하고 있습니다. 우리는 "오늘 밤 싸워



라"라는 사치가 없습니다. 해군 네트워크는 오늘 싸움에 있습니다.

2018년 국방 전략의 발간은 자원을 조율하고 노력을 동원했으며 우리가 대권력 경쟁 (GPC)과 관련된 우리 국가가 직면하고 있는 괴로운 문제에 대해 명확하게 지시했습니다. GPC는 단순한 유행어가 아닙니다. 그것은 현재뿐만 아니라 장기적으로도 현실입니다. 그것은 민주주의와 권위주의 정권 사이의 미래에 대한 두 가지 비전 사이의 도전입니다. 내비게이션의 자유, 시장과 아이디어에 대한 접근, 그리고 강압적인 구속 사이에서. 인터넷의 개방성과 취약성은 이 경쟁에서 중요한 역할을 합니다. 또래의 적들과 떠오르는 반란주의 국가들이 국제 규범을 훼손하고 지역 안정성을 위협하고 있습니다."

나는 21세기 대권력 갈등의 시작 라운드, 특히 해양 영역에 영향을 미치는 분쟁이 전자기, 우주 또는 사이버 영역에서 시작될 것이라고 확신합니다. 해군이 싸우고 이기려면 해군 네트워크는 이러한 공격에서 살아남아 "상처와 싸울" 수 있어야 합니다. 우리 국민은 이러한 타격을 견디기 위해 훈련과 훈련을 받아야 합니다. 이 경연은 경쟁과 갈등의 연속성을 포괄합니다. 우리는 네트워크가 이미 긴밀히 접촉하고 지속적인 조사와 공격을 받고 있는 "평화 시간 작전"의 일상적인 경쟁에서 대회에서 우승해야 합니다. 그렇지 않으면 위기와 치명적인 전투에서 심각한 불이익을 받게 될 것입니다.

더글러스 맥아더 장군은 전쟁 실패의 공통 분모는 "너무 늦었다"는 두 단어로 요약 될 수 있다고 주장했다. 적의 의도를 이해하기에는 너무 늦었고, 준비하기에는 너무 늦었고, 동원하기에는 너무 늦었고, 억제하기에는 너무 늦었고, 동맹과 파트너와 함께 서기에는 너무 늦었고, 가장 중요한 것은 먼저 행동하기에는 너무 늦었습니다. 나는 동의합니다.

나는 이점이 먼저 움직이는 쪽에 있다고 믿습니다. 완전히 경쟁이 치열한 전장에서 싸우고 승리 할 때 전체 스펙트럼 정보 전쟁에서 승리하려면 "선발자 이점"을 모든 작전의 기반으로 받아 들여야 합니다.

먼저 움직이는 것은 결정과 행동이라는 두 가지 장점이 있습니다. 각각은 운동 무기와 비 운동 무기의 사용에 큰 영향을 미칩니다. 오늘날의 강력한 적들과의 경쟁에서 승리하려면 우리의 전술은 두 가지 요소를 포괄해야 합니다. 그러나 해군의 모든 측면이 스펙트럼 및 프로토콜과 관계없이 글로벌, 모바일, 보안 무선을 통해 연결 및 네트워크로 연결되지 않은 경우 이 중 어느 것도 불가능합니다. 탄력적이고 강화 된 해군 네트워크 일수록 적군이 위기 상황에서 네트워크를 저하시키는 것이 더 어려워집니다. 우리는 해군 네트워크가 치명적인 전투 중에 함대에게 중요한 이점을 유지하도록 해야 합니다.

끊임없이 변화하는 기술 생태계에서 우리는 정보, 지식, 지적 재산, 국가 안보 및 주권을 보호하기 위해 고군분투하고 있습니다. 해군 전체에서 많은 사람들이 현재 상황의 심각성을 파악하고 있습니다. 우리는 위대한 권력 경쟁에서 승리하기 위해 필요한 변화를 만들기 위해 "모든 손" 응답이 필요합니다.



GPC는 전략 계획이 정적으로 유지 되기에는 너무 역동적입니다. 미래의 사령관은 자신의 시계에 나타날 도전을 해결하기 위해 필요에 따라 조정하거나 수정해야 합니다. 우리는 중요한 이해 관계가 바다에 단단히 묶여 있는 해양 국가입니다. 해병대와 해안 경비대의 동료들과 함께 우리는 전략적 경쟁자들의 도전으로부터 이러한 이익을 보호해야 합니다.

전략 계획 2020-2025의 근본적인 목적은 "We Get It"을 보여주는 것입니다. 우리는 이를 처리 할 계획을 가

TJ White

Vice Admiral, 미 해군

사령관, 미 함대 사이버 사령부 / 미 TENTH 함대

페이지 1

내용

| | |
|----------------------------------|----|
| 사령관의 서문..... | 1 |
| 요약..... | 3 |
| 전략 계획 2020-2025의 기초..... | 4 |
| 중요한 가정..... | 5 |
| 우리의 지속적인 책임..... | 5 |
| 전략적 환경..... | 6 |
| 합동 군, 동맹국 및 파트너..... | 7 |
| 조직 환경..... | 7 |
| 새로운 개념 및 기술..... | 8 |
| 우리의 사명, 비전 및 지도 원칙..... | 9 |
| 목표 1 : 네트워크를 전쟁 플랫폼으로 운영합니다..... | 11 |
| 목표 2 : 함대 암호 전쟁 수행..... | 13 |
| 목표 3 : 전투 능력 및 효과 제공..... | 15 |
| 목표 4 : 해군 사이버 부대 가속화..... | 17 |
| 목표 5 : 해군 우주 사령부 설립 및 성숙..... | 18 |
| 마무리..... | 20 |
| 용어집..... | 21 |





정보 전쟁 (IW)은 항해 시대부터 미국 해군 작전의 일부였습니다 (매우 낮은 데이터 속도에도 불구하고). IW는 해군이 미드웨이 전투에서 승리하도록 도왔고 대서양 전투에서 U- 보트를 이기고 수십 년 동안의 소련 해군과의 경쟁에서 중요한 역할을 했습니다.

21 세기 정보화 시대에 사이버 공간은 도메인으로 등장하여 우리가 싸우려는 가정을 근본적으로 바꾸었습니다. 우리의 장기적인 전략적 경쟁자들에 대한 폴 스펙트럼 IW는 우리가 정기적으로 우리의 가정에 도전 할 것을 요구하는데, 이것이 바로이 전략 계획을 업데이트하기 위해 한 일입니다.

전략 계획의 비전은 상호 관련된 세 가지 주요 요소로 구성됩니다.

- 전체 스펙트럼 정보 전쟁에서 선점자 이점 보장
- 완전히 경쟁하는 전장에서 싸우고 승리하기
- 현대화 및 혁신 촉진

전략 계획 : 2015-2020에 대한 우리의 평가는 GPC로의 전환과 IW의 성숙을 반영하기 위해 몇 가지 사소한 수정 후에도 비전을 발전시키는 데 5 가지 전략적 목표가 관련성이 있음을 확인했습니다. 수정 된 전략적 목표는 다음과 같습니다.

- 목표 1 : 네트워크를 전쟁 플랫폼으로 운영합니다. 우리는 해군 네트워크, 통신 및 우주 시스템을 안전하게 운영, 유지, 방어 및 조종하여 군대가 필요할 때 언제 어디서나 가용성을 보장해야합니다. 네트워크는 타락한 상태에서 싸울 수 있어야합니다. 또는 전쟁 목표를 달성하기 위해 우리가 "싸움 상처"라고 부르는 상황에서 싸울 수 있어야합니다.
- 목표 2 : 함대 암호 전쟁 수행. DMO (Distributed Maritime Operations)에 대한 기여의 일환으로 SIGINT (Distributed Signals Intelligence) 작전 (DSO)에서 기술과 능력을 확장하고 향상시키고 함대 수준의 전쟁에 대한 해군의 새로운 강조를 지원합니다.
- 목표 3 : 전투 능력 및 효과 제공. 해군 지휘관이 DMO를 지원하기 위해 자신의 능력을 완전히 활용할 수 있도록 사이버 공간을 통해 전투 능력 및 효과 (이동, 기동 및 화재)를 제공하는 능력을 확장하십시오.
- 목표 4 : 해군의 사이버 부대 가속화. 지속적인 참여 및 전진 방어의 요구를 충족하기 위해 해군 사이버 팀의 역량과 역량을 키우십시오. 국가의 사이버 임무 군을 발전시키면서 해군 목표물을 서비스하는 함대 사이버 작전 팀에 대한 요구 사항을 개발할 것입니다.

10년 전, 우주에서의 전쟁(운동 및 비 운동)은 20년 후의 전쟁 게임에서만 실행되었습니다. 미래는 지금입니다. 우주 전쟁은 더 이상 공상 과학의 주제가 아니며 해군은이 새로운 현실에 맞서야합니다. 따라서 이 계획에는 우주, 사이버 공간 및 전자기 스펙트럼(EMS) 간의 증가하는 수렴을 활용하기 위해 우주 영역에서 이 사령부의 추가 책임을 반영하는 전략적 목표가 포함됩니다.

- 목표 5 : 해군 우주 사령부 설립 및 성숙. 우리의 목표는 치명성, 준비성 및 능력에 중점을 두고 해저에서 우주까지 해상 우월성을 유지하는 것입니다. 미 우주 사령부의 재 수립과 미 우주군의 창설과 함께, 우리는 모든 영역 작전을 지원하기 위한 포괄적인 우주 능력의 가능한 최상의 통합을 제공하기 위해 다시 집중해야 합니다.

이 계획의 뒷부분에서 자세히 설명하는 5 가지 전략적 목표는 시작에 불과합니다. 전략 계획 2020-2025는 또한 일련의 후속 구현 및 캠페인 계획의 기반이 될 것입니다.

오늘날 해군은 그 어느 때보다 IW 기술이 필요합니다. 우리는 이 10년이 진행됨에 따라 그 필요성이 더욱 커질 것을 예상해야 합니다. 우리는 사이버 공간과 모든 C2(명령 및 제어) 환경을 통해 "킬 체인"이 효과적으로 작동하도록 해야 합니다. 우리는 우리 자신을 보호하면서 적의 능력과 의도를 알아야 합니다. 우리는 그들이 어디에 있고 무엇을 하고 있는지 항상 알아야 합니다. 우리는 그들의 의사 결정 과정을 무너뜨리고 우리 자신을 보존해야 합니다. 우리는 준비에 실패 할 수 없습니다.

3 페이지



The history of failure in war can almost be summed up in two words: 'Too late.' Too late in comprehending the deadly purpose of a potential enemy; too late in realizing the mortal danger; too late in preparedness; too late in uniting all possible forces for resistance, too late in standing with one's friends. Victory in war results from no mysterious alchemy or wizardry but depends entirely upon the concentration of superior force at the critical points of combat.

~ General Douglas MacArthur, United States Army, 1940



전쟁 실패의 역사는 '너무 늦었다'는 두 단어로 요약 될 수 있습니다. 잠재적 인 적의 치명적인 목적을 이해하는 데 너무 늦었습니다. 필멸의 위험을 깨닫는 데 너무 늦었습니다. 준비가 너무 늦었습니다. 저항을 위해 모든 가능한 힘을 결합하는 데 너무 늦었고 친구와 적에게는 너무 늦었습니다. 전쟁에서의 승리는 신비한 연금술이나 마법의 결과가 아니지만 전적으로 전투의 중요한 지점에서 우월한 힘의 집중에 달려 있습니다.

~ 1940년 미군 더글러스 맥아더 장군

창설 이래로 6 척의 원래 프리깃부터 오늘날의 300 척 이상의 선박에 이르기까지 해군은 국가에 봉사하기 위해 신뢰할 수 있고 안전하며 적절한 정보가 필요했습니다. 우리의 선박과 항공기가 평화와 전쟁에 배치됨에 따라 정보 경쟁은 점점 더 중요해지고 있습니다.

해군 전체에서 선박과 선원은 스펙트럼을 통해 연결되어 상상할 수 없었던 속도로 데이터를 생성하고 소비합니다. 기술이 발전함에 따라 우리의 전투 시스템은 신뢰할 수 있는 정보에 완전히 의존하게 되었습니다. 현재 시대의 특징은 분산 된 센서 전면에 걸쳐 아날로그와 디지털 시스템 간의 수렴이 가속화된다는 것입니다. 여기에는 데이터 수집, 정보 과학 및 자율적인 의사 결정에 접근하는 학습이 포함됩니다.

5 가지 전략적 목표의 배경과 동인을 이해하려면 2020-2025년 전략 계획의 기반이 되는 지적 기반을 구성하는 요소를 검토하는 것이 중요합니다. 요소는 사령부의 전반적인 가정, 지속적인 책임, 동맹과 파트너를 포함한 전략적 환경 평가, 조직 환경, 이번 10년이 진행됨에 따라 고려해야 할 새로운 개념과 기술, 우리의 사명, 비전 및지도 원칙으로 구성됩니다.

"We look forward to advancing our long-standing cryptologic partnership as we ensure the Fleet is best positioned to meet the demands of Great Power Competition, and we maintain superiority across the maritime domain and littorals. In particular, there are great opportunities ahead as we operate as Distributed SIGINT Operations teammates, advance our expertise on the operations and capabilities of our strategic competitors, and leverage all partnerships to our warfighting advantage."

- Lieutenant General Lori Reynolds, USMC, Deputy Commandant for Information

4 페이지

STRATEGIC ALIGNMENT

Strategic Plan 2020 - 2025 is consistent with and aligned to the following higher strategic guidance:

- National Security Strategy (2017)
- National Cyber Strategy (2018)
- National Strategy to Secure 5G (2020)
- National Defense Strategy (2018)
- Department of Defense Cyber Strategy (2018)
- Department of Defense Digital Modernization Strategy (2019)
- Defense Space Strategy (2020)
- Department of the Navy Information Superiority Vision (2019)
- U.S. Cyber Command Vision (2018)
- Chief of Naval Operations FRAGO 01/2019: Maintaining Maritime Superiority (2019)
- Naval Doctrine Publication 1, Naval Warfare (2020)

포괄적 인 가정

모든 전략 기획자에게는 가정이 중요합니다. 그들은 모든 계획이 수행되는 현실을 반영합니다. 가정은 명확하게 기술되어야 하며 여전히 유효한지 확인하기 위해 정기적으로 재검토해야 합니다. 그렇지 않다면 가정은 계획의 가장 약한 요소가 됩니다. 다음 가정은 전략 계획의 기초입니다.

- 해군의 해상 전쟁에 대한 DMO (Distributed Maritime Operations) 개념은 IW가 DMO의 중요한 원동력이 되는 대규모 권력 충돌시 해상 우월성을 보장하려는 해군 계획의 핵심입니다.

- DMO는 AC2 (Assured Command and Control), BA (Battlespace Awareness) 및 IF (Integrated Fire)로 뒷받침됩니다.
- 미국 사이버 사령부 교리는 Defend Forward, Persistent Engagement 및 Joint Cyber Warfighting Architecture (JCWA)에 중심을 두고 있습니다.
- 중국은 향후 세계적 우위를 달성하기 위해 단기적으로 인도-태평양 지역 해제모니와 미국의 이주를 추구하는 군사 현대화 프로그램을 계속 추구 할 것입니다.
- 러시아는 북대서양 조약기구를 분쇄하기 위해 정부, 경제, 외교적 결정 측면에서 주변 국가에 대한 거부권을 추구합니다.

우리의 지속적인 책임

현대 해전의 폭, 범위, 치사율 및 화력은 지난 100년 동안 극적으로 증가했습니다. 해전이 한때 해수면과 그 바로 위의 공중에 국한된 해전이었던 곳에서 오늘날 해군은 해저에서 우주로, 모든 지역, 사이버 공간 및 전자기 스펙트럼에서 활동합니다. IW는 해군의 주요 전쟁 지역 중 하나입니다. 그것은 다른 해전 지역의 성공에 필수적이며, 실제로 필수 불가결합니다. Fleet Cyber Command / TENTH Fleet (FCC / C10F)가 전체 스펙트럼 IW를 수행하고 다른 전쟁 지역을 활성화하려면 AC2, BA 및 IF를 제공 할 수 있어야 합니다. 이는 평화, 위기 또는 분쟁의 시기와 C2 환경에서 우리의 지속적인 책임입니다. AC2를 실행하는 해군 IW 선원, BA 및 IF 임무는 모든 해양 적의 위치와 의도에 대한 정확한 정보를 일관되게 유지하고 성공적인 표적화를 가능하게하고 이러한 위협에 대한 교전 및 패배를 가능하게하는 함대의 능력에 점점 더 없어서는 안될 역할을 합니다. 이 사령부의 모든 구성원은 이러한 결과를 이해하고 전달하는 데 기여해야 합니다.

AC2는 배치 된 유닛과 해안에 있는 부대간에 중단없는 전 세계 통신을 가능하게하기 위해보다 강력하고 보호되며 탄력적이며 안정적인 정보와 네트워크 인프라가 필요합니다. 해군의 정보 인프라는 중요한 전투 정보 및 평가를 전송, 공유, 저장, 보호 및 전파하기 위해 전자기 스펙트럼의 보안 세그먼트에서 필수 네트워크 및 데이터 서비스를 유지해야합니다.

BA는 우리의 적과 운영 환경에 관한 정보를 신속하게 감지, 수집, 처리, 분석, 평가 및 전파하기 위한 향상된 정보 콘텐츠, 고급 수단이 필요합니다. 우리의 정보 콘텐츠는 거의 모든 결정을 내리는 기반이되어 우리 군대가 적군을 목표로하고 교전하는 행동을보다 효과적으로 조종하고 조정할 수 있도록 합니다.

IF 기능은 두 가지 주요 전투 기능에 기여합니다. 첫 번째는 킬 체인의 왼쪽 행동에 대응하기 위한 사전 조치를 취하여 적의 화재를 방해하거나, 거부하거나, 물리 치는 것입니다. 두 번째는 AC2 및 BA 기능의 절정을 통해 우리의 운동 및 비 운동 화재를 향상시키는 것입니다. Navy IF 기능은 전자전 및 공격 사이버 효과에서 확장되는 이점을 활용하여 운동 및 비 운동 무기를 보완합니다.

AC2 및 BA는 함대의 표적 선택 및 할당 프로세스에 단단히 포함되어야 합니다. 그런 다음 원하는 치명적 또는 치명적이지 않은 효과를 달성하기 위해 표적을 참여시키는 적절한 수단 (IF)을 일치시킬 수 있습니다. 재밍, 공격적 사이버 공간 작전 또는 지향성 에너지 무기를 포함하여 이에 국한되지 않는 기존의 "목표 철제"화재 또는 비운동적 화재를 사용하든 우리는 이러한 수단을 해군 전쟁에서 전략 및 작전 요구 사항을 충족하도록 고려 할 것입니다.





통합 화재를 진전시키는 정보 전쟁

5 페이지



전략적 환경

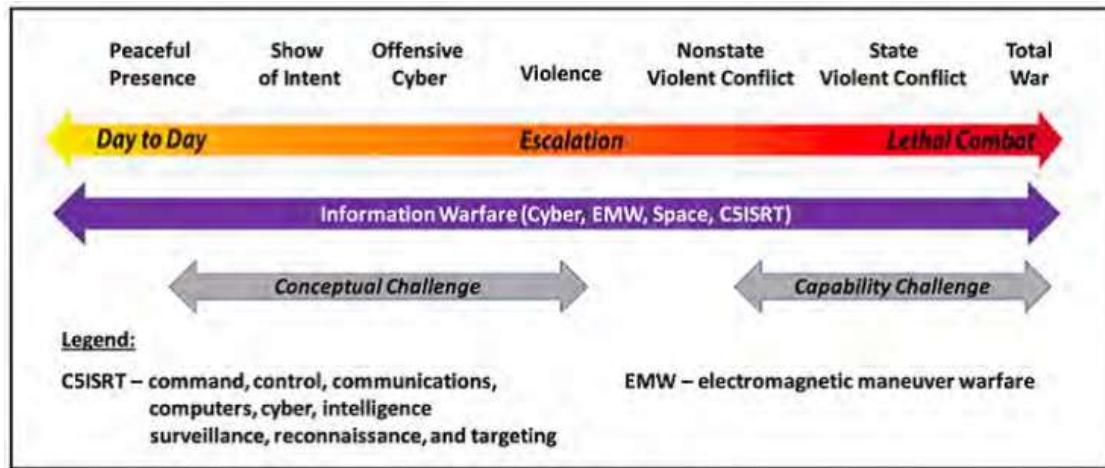
지구 표면의 70 %가 물로 덮여 있으며 지구 인구의 70 % 이상이 해안에서 100 해리 이내에 살고 있습니다. 세계 무역의 90 % 이상이 해상으로 이동하는 반면, 전 세계 통신의 99 %가 수중 케이블을 통해 이동합니다. 인류는 더 많은 공간을 차지하고 세계는 점점 작아지고 있으며 이제 우리는 그 어느 때보다 기술을 통해 더 많이 연결됩니다. 국제 시장에 대한 우리의 접근은 동료 또는 근거리 경쟁자로부터 해로를 보호하기 위한 해상 전력에 달려 있습니다. 전략적 환경은 모두 해양 영역에 관한 것입니다. 이것이 미국이 시장에 대한 접근을 보장하고 우리의 아이디어, 이상 및 정체성의 주권을 확보하기 위해 항해의 자유를 보장하기 위해 해군이 필요한 이유입니다.

이러한 환경에서 우리의 적들은 지속적으로 사이버를 수행하고 운영에 영향을 주어 우리의 생활 방식을 방해합니다. 예를 들면 선거 위협, 민감한 방어 정보 도용, 기업 스파이 행위 및 개인 식별 정보의 대규모 도난이 있습니다. 해군은 이러한 활동을 방어하고 대응하려는 미국의 노력에 필수적입니다.

NDS는 Great Power Competition의 재 등장이 미국의 번영과 안보의 핵심 과제라고 말합니다. 이 경쟁은 전 세계적이며 모든 영역에 참여하고 있으며 해군은 선진적이고 민첩하며 준비가되어 있어야 합니다.

Naval Doctrine Publication 1, Naval Warfare는 GPC를 경쟁과 갈등의 연속체로 묘사합니다. 연속체에는 평시 동안 수행되는 일일 작전, 위기로의 확대, 강력한 힘의 적에 대한 치명적인 전투 전투가 포함되며 전체 스펙트럼 IW는 연속체에서 일관되게 수행되었습니다.

NDS는 또한 우리가 중국 및 러시아와의 장기적인 전략적 경쟁에 있음을 분명히하지만 이 경쟁은 냉전과는 다릅니다. 그 오랜 투쟁에서 우리의 전반적인 전략은 우리가 사실상 경제적 관계가 없는 또 다른 세계 강국인 소련을 군사적, 외교적으로 포함하는 것이었습니다. 오늘날 우리가 직면 한 장기적인 경쟁은 민주주의와 권위주의 정권, 항해의 자유, 공유 된 세계 시장에 대한 접근 사이입니다. 우리의 장기 전략적 경쟁자들은 국제 질서를 바꾸기 위해 전략적 사이버 활동을 실행하고 있습니다. 이것은 포기하지 않을 것입니다. 우리의 전략적 경쟁자들은 그들이 우리와 경쟁 할 수 있도록 우리가 "게임을 하는"방법을 배우기 위해 수년간 우리를 연구 해 왔습니다. 그들의 움직임에 대응하기 위해 우리는 그들의 게임을 배우고, 그들이 어떻게 플레이하는지 연구하고, 우리의 방식대로 플레이해야합니다.



경쟁-분쟁 연속체 (출처 : Naval Doctrine Publication 1, Naval Warfare, 2020 년 4 월)

페이지 6

이것이 왜 중요한가요? 역사적으로 국가의 권력을 약화시키기 위해서는 영토에 초점을 맞춘 명백한 무장 공격이나 물리적 침략이 필요했습니다. 그것이 항상 가능하고 앞으로도 계속 될 것이지만, 기술은 우리의 적들에게 전통적인 군사력 없이도 목표를 달성 할 수 있는 능력을 제공했습니다. 현재 우리의 적들은 우리를 사이버 공간에 참여시키고 있으며 비용은 누적됩니다. 각 침입, 해킹 또는 유출은 그 자체로 전략적으로 결과가 아닐 수 있지만 복합적인 효과는 전쟁 행위로 간주되는 것과 같습니다.





IW Across the Global Continuum of Competition-Conflict

장기적인 전략적 경쟁을 배경으로 사이버 도메인의 진화하는 특성이 있습니다. 지역 권력과 독립 행위자들은 그들의 이익을 증진하기 위해 점점 더 사이버 공간을 이용할 것입니다. 그들은 사이버 활동의 비기 인적 특성과 적시에 책임을 집행하는 데 어려움이 있기 때문에 더 큰 위험을 기꺼이 받아들이고 공격에 더 뻔뻔스러울 수 있습니다. 정보 영역에서 이러한 악의적인 활동이 즉각적으로 발생한다는 것은 이 도전이 현재의 강력한 공격자들뿐만 아니라 가까운 미래에 우리에게 직면 할 것이라는 것을 의미합니다. 해군은 우리를 위협하는 지역 또는 비 국가 행위자들에 맞서기 위해 군대를 배치하고 장비해야 합니다.

합동 군, 동맹 및 파트너

미국의 해군 서비스인 해군, 해병대 및 해안 경비대는 동맹국과 파트너의 지원, 협력 및 귀중한 기여 없이는 전 세계적으로 운영 할 수 없습니다. 우리의 결합된 힘은 확립 된 국제 규범에 맞서기 위해 강압과 협박에 의존하는 장기적인 전략적 경쟁자보다 구조적 이점을 제공합니다. 이러한 이유로 우리의 적들은 우리의 이점을 약화시키는 저비용, 낮은 위험 및 효과적인 방법이 사이버 도메인에서 악의적인 행동을 하는 것임을 알고 있습니다. 사이버 공간에서 그들은 작전을 가릴 수 있고 잘못된 정보, 불일치 및 분열의 원인이 될 위험을 최소화 할 수 있습니다. 일상적인 경쟁에서 성공하기 위해 우리는 합동 세력에 참여하는 것처럼 동맹국과 파트너와 원활하게 참여해야 합니다.

위기나 치명적인 전투가 발생하는 경우, 우리 동맹국과 파트너는 우리의 전략적 중심입니다. 우리는 글로벌 IW 캠페인 기간 동안 연합으로서 협력과 상호 운용성을 구축하고 유지할 수 있도록 동맹과 파트너십을 확장하고 강화해야 합니다. 해상력의 지역적 균형을 우리에게 유리하게 유지하거나 회복 할 수 있는 것은 우리의 가장 강력하고 유능한 동맹국과 파트너들과 함께 할 때입니다.

조직 환경

우리가 운영하는 조직 환경은 국제 전략 환경만큼이나 역동적입니다. 이전 전략 계획이 발표된 이후 조직 환경에 많은 변화가 있었습니다. 우리나라는 미군 사이버 사령부 (USCYBERCOM)를 하위 통합 사령부에서 전투 사령부로 승격하고, 미 우주 사령부 (USSPACECOM)를 재건하고, 우주에 초점을 맞춘 새로운 서비스를 생성하고, 전략을 강조하기 위해 미 태평양 사령부로 이름을 변경했습니다. 인도양 지역의 중요성, 제2 함대 재건. 우리는 앞으로 더 많은 변화를 예상해야합니다.

FCC는 해군 정보 네트워크 운영, 공격 및 방어 사이버 공간 운영, 우주 운영 및 신호 정보를 담당하는 제2 사령부로 해군 작전 책임자에게 직접보고합니다. 운영상 FCC는 미국 사이버 사령부에서 해군 구성 요소 및 사이버 사령부 (JFHQ-C 해군), 미국 우주 사령부에서 해군 구성 요소, 국가 안보국 / 중앙 보안 서비스의 해군 서비스 암호화 구성 요소 사령관 역할을 합니다.

FCC는 또한 미국 전략 사령부의 해상 구성 합동 사령관인 함대 사령부를 통해 미국 전략 사령부에 대한 핵 명령 및 통제 및 통신 (NC3) 기능을 실행합니다. 위대한 권력 갈등이 전략 핵무기로 무장한 국가를 포함 할 가능성이 있다는 사실을 결코 잊지 말아야합니다. Nation의 핵 트라이어드 해저 다리의 지속적인 생존에 대한 우리의 주요 기여는 NC3 네트워크를 유지, 운영 및 방어하는 것입니다.



Maryland National Guard cyberwarfare operators support Exercise Hedgehog 2018 in southern Estonia, May 2018. Army National Guard photo.

USS Ronald Reagan and the Japan Maritime Self Defense Force JS Izumo conduct bilateral exercises in the South China Sea. US Navy photo.

HMS Queen Elizabeth in the Atlantic Ocean. U.S. Navy photo.

페이지 7

US TENTH Fleet은 FCC의 제3 대 작전 명령으로, 다른 함대 사령관과 같은 태스크 포스 구조를 통해 임무를 수행합니다. 해군의 다른 번호가 매겨진 함대와는 달리 C10F는 모든 영역 (우주, 사이버, 해상, 항공, 육상 및 정보)에서 운영되는 전 세계적으로 운영되는 유일한 함대입니다. 우리는 신호 정보, 통신, 사이버 공간 및 우주 작전, 전자전을 담당하는 해군의 저명한 IW 전문가입니다. 우리의 핵심은 적대적 사고 방식을 가진 전투원으로서, 모든 지휘 및 통제 환경에서 모든 전쟁 영역에서 경쟁력 있는 결과를 제공합니다. 매일 지속, 무장 정찰, 비행 분대, 사이버 공간 "FOD 워크 다운", 화재 감시, 순찰 순찰, PACFIRE를 중심으로 구성됩니다.

할당 된 USCYBERCOM 서비스 JFHQ-C로서, 우리는 할당 된 자리 전투원 명령에 대해 전체 스펙트럼 사이버 공간 작전의 지역 조정 권한을 실행합니다. 최근 FCC는 합동 우주 커뮤니티 내에서 해군 임무를 수행하기 위해 해군 우주 사령부 역할을 맡았습니다.

"The U.S. Coast Guard is fully committed to leveraging cyberspace operations under the Distributed Maritime

Operations (DMO) concept and values the Navy leadership in this domain to protect and project the sovereignty of our Navy across the global maritime commons. Working as a team, the Naval Services must employ cyberspace operational concepts and capabilities to deliver effects that will allow us to fight and win in Great Power Competition.” - Rear Admiral Mike Ryan, USCG, Coast Guard Cyber Command

새로운 개념과 기술

새로운 개념과 기술이 IW의 미래를 형성 할 것입니다. 일부는 오늘날 미성숙 한 상태에 있고 다른 일부는 지평선에 있습니다. 우리는 그들의 진행 상황을 모니터링하고, 신속하게 활용하고, 적을 불리한 전술 상황 (TACSI)에 유지하기 위해 전술, 기술 및 절차 (TTP)를 조정해야합니다.

전방 및 지속적인 참여를 방어하십시오. 최근 채택 된 이러한 전략적 개념은 사이버 도메인에서 운영하기 위한 미국 사이버 사령부의 원칙의 핵심입니다. 그러나 그들은 1775 년부터 해군 문화의 중심이었습니다. 우리는 대웅 전망에서 전진을 방어하고 가상 항구에서 사이버 능력을 이동시키고 오늘날의 현실과 일치하는 자세를 취하는 지속적인 세력으로 전환했습니다. 해군은 입국을 통해 방어하지 않고 우리 나라를 방어하기 위해 전진 배치됩니다. 사이버 공간의 고유 한 특징은 상호 연결성과 지속적인 접촉입니다. 이 조합은 지속적인 행동을 요구합니다. 이러한 개념이 완전히 효과적이려면 동맹국 및 파트너와 긴밀하게 협력하는 것이 중요합니다.

인공 지능 (AI) 및 기계 학습 (ML). AI와 ML의 발전은이 나라와 우리의 강력한 경쟁자들에게도 사이버 공간에서 기회와 도전을 창출하고 있습니다. 이 사령부는 이러한 발전을 인식하고 전체 스펙트럼 IW에 이점을 제공 할 수 있는 혁신적인 AI / ML 개념을 기꺼이 실험해야합니다. 이 두 가지 신흥 기술은 빠르게 발전하고 있으며, 우리는 JAIC (Joint Artificial Intelligence Center) 및 기타 유사한 조직과 협력하여 이러한 과제를 해결하고 이러한 기술을 채택해야합니다.





8 페이지

양자 컴퓨팅. 우리는 양자 컴퓨팅이 사이버 공간에서 유망한 새로운 기회와 잠재적으로 우리가 암호화 한 모든 비밀을 열 수 있을 만큼 실용적이 되는 날을 준비해야 합니다. 해군은 점점 더 중요해지는 이 분야에서 미군이 다른 강대국보다 앞서 있도록 보장하기 위한 국방부의 노력에서 중심적인 역할을 할 수 있습니다.

클라우드 컴퓨팅. 클라우드 컴퓨팅은 네트워크 공간을 줄이고 컴퓨팅 성능과 협업 능력을 높일 수 있습니다. 우리는 클라우드 컴퓨팅의 효율성을 프로세스에 통합하여 지휘관의 의사 결정주기를 가속화하고 경쟁과 갈등의 연속에서 선점자 이점을 실현해야 합니다. 클라우드에서 해군 데이터를 보호하기 위한 방어 수단을 개발해야 합니다.

5G. 5 세대 무선 기술은 향후 10 년 동안 미국의 안보와 번영의 주요 동력이 될 것입니다. 그러나 5G는 또한 공격자와 기타 악의적인 행위자가 악용 할 수 있는 다양한 새로운 위험과 취약성을 제시합니다. 5G 우월성과 공급망 보안을 위한 경쟁은 6G가 곧 다가오는 10 년 동안 주요 "준비 경쟁"이 될 수 있습니다.

우주 기반 사이버 공간 운영. 우주 기반 서비스는 반세기 이상 해군 작전의 중심이었습니다. 어떤 형태의 우주 지원 시스템이나 서비스 없이 해군이 작전을한다고 상상하는 것은 거의 불가능합니다. 우리의 적들은 우주가 군사 작전에 유리할 수 있다는 것을 오랫동안 깨달았습니다. 그들은 자신의 능력을 개발하고 배치하면서 우리의 능력에 대응하기 위해 시스템을 개발하고 배치하고 있습니다. 국방부의 진화하는 우주 아키텍처는 강력한 권력 갈등이 제공하는 위협을 처리해야 합니다. 따라서 우리는 경쟁과 갈등의 연속체에서 새로운 사이버 기능을 실험해야 합니다.

해양 지원 사이버 공간 운영. 기술 개발의 역사는 지상에서 발명 된 모든 것들이 결국 해양 영역 (무선, 레이더, 컴퓨터, 원자력 등)으로 향하고 있음을 말해줍니다. 사이버 공간 작전, 특히 사이버 보안 및 사이버 방어에서도 마찬가지입니다. 우리는 적보다 먼저 적절한 해양 기반 사이버 공간 운영을 개발하고 배치 할 준비가되어 있어야 합니다.

"Colonel John Boyd said it best: 'Those who recognize change, understand change and exploit change to their advantage, win!' We are living in a constant state

of change. Because of our great people, we have the advantage to change quicker than our adversaries. Again from Boyd: 'we must focus on people, ideas and things, in that order!'"

- Major General Matthew G. Glavy, USMC,
Commander, Marine Corps Forces Cyberspace

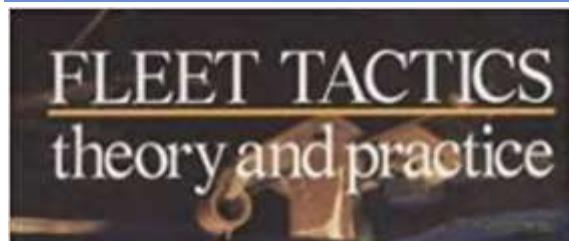
우리의 사명, 비전 및 지침 원칙

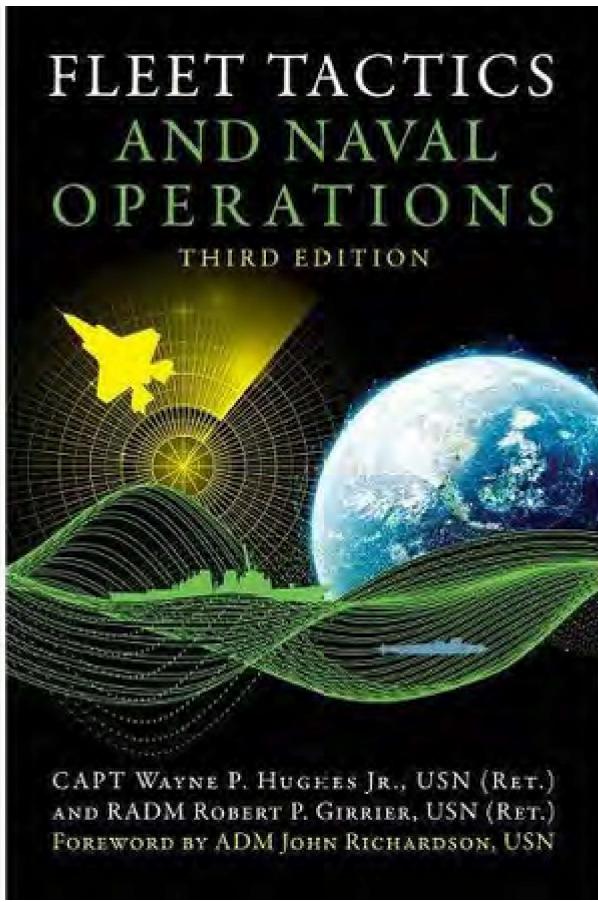
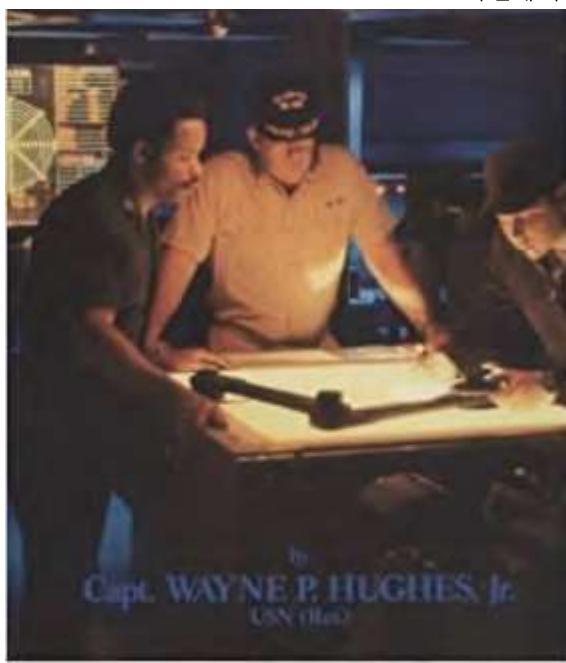
우리의 임무는 사이버 공간을 통과하고 사이버 공간에서 모든 해군의 전투 영역에서 행동의 자유를 보장하고 이를 거부하는 데 필요한 사이버 공간 작전 활동의 전체 연속체를 계획, 조정, 통합, 동기화, 지시 및 수행하는 것입니다. 적. 전체 임무의 일환으로 해군의 네트워크를 운영 및 방어하고 관련성 있고 실행 가능한 정보 및 감시 데이터를 생성하는 동시에 전 세계에 배치 된 작전 부대에 통신을 제공하는 신흥 및 레거시 해군 우주 시스템을 계획 및 운영합니다.

우리의 비전에는 세 가지 주요 요소가 있습니다.

- 1) 선점자 우위 확보
- 2) 경쟁이 치열한 환경에서의 싸움과 승리
- 3) 현대화 및 혁신 촉진

풀 스펙트럼 정보 전쟁에서 선점자 우위 보장. 그의 고전적인 책 *Fleet Tactics*에서 고인 Wayne Hughes 대위는 "효과적인 우선 공격"이라는 강력한 말로 해군 전쟁의 본질을 요약했습니다. Hughes의 책은 센서, 무기 및 플랫폼 간의 역사적이고 지속적인 관계를 설명했습니다.



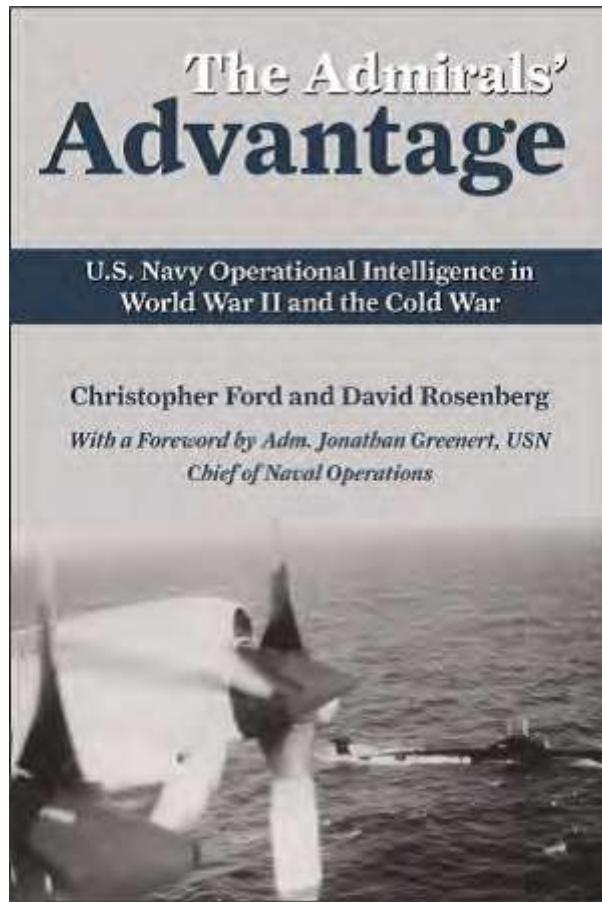


이번 10년 동안 새로운 무기, 센서 및 플랫폼이 함대에 진입함에 따라 우리의 과제는 강력한 적의 해군과 싸우라는 요청이 있을 경우 함대가 먼저 효과적으로 공격 할 수 있도록 전술을 개선하는 것입니다. Wargames, 연습 및 실험은 Hughes의 격언을 확인하고 MacArthur 장군의 관점을 강화했습니다. 이 점은 먼저 움직이는쪽에 있습니다.

선발자 이점의 두 가지 주요 구성 요소는 결정과 행동으로, 운동 무기와 비 운동 무기 사용에 큰 영향을 미칩니다. 두 유형의 무기에 대한 해군의 새로운 전술은 해군이 미래의 전투에서 승리하기 위해 이러한 구성 요소를 포함해야합니다. 우리는 해전에서 이 혁명의 선두에 서게 될 것입니다.

전선의 경쟁력을 신경 채우는 것은 중요합니다. 그러나 전선에서 전투를 벌이기 위해서는 해군이 사용할 수 있는 것보다 빠르고 효과적인 킬 체인이 필요합니다. 치명적인 전투 중에 기동과 발사(운동 및 비 운동)를 동기화해야 합니다. 우리는 가장 유리한 TACSI를 유지해야 합니다. 해군이 먼저 효과적으로 공격하려면 (선발자 이점을 활용하기 위해) 서로 다른 C2 환경에서 제시하는 문제를 해결하는 전술을 개발해야 합니다.

우리는 킬 체인이 효과적이고 함대 사령관이 그에 따라 부대를 조종 할 수 있도록 경쟁이 치열한 C2 환경에서도 전략적 경쟁자의 해군 병력의 위치와 이동에 대한 지속적인 인식을 제공해야 합니다. 전 세계적으로 배치 된 소련 해군에 대한 냉전에서의 우리의 경험은 비전을 알려줄 것입니다. Christopher Ford와 David Rosenberg의 *The Admirals' Advantage*에서 말했듯이 해군은 분산 된 데이터 노드를 기반으로 구축 된 강력한 글로벌 정보 공유 네트워크를 개발하여 전 세계 해양 감시 정보 시스템(OSIS)을 구축하는 데 앞장 섰습니다. 1980 년대 말까지



위기 상황에서 적의 목표는 킬 체인을 저하시키고 파괴하는 것이며, 우리도 똑같이 할 것입니다. 이러한 이유 때문에 “평화시” 동안 네트워크 전쟁 플랫폼의 무결성을 유지하는 것이 매우 중요합니다. 우리가 네트워크를 운영 및 방어하고 평시 동안 사이버 보안을 강조할수록 적이 이를 저하시키는 것이 더 어려워집니다. 위기. PE (Persistent Engagement)는 일상적인 작전 중에 우리를 경쟁에서 유지하고, PE의 복합 효과는 시간이 지남에 따라 해군의 네트워크 전쟁 플랫폼이 위기 및 치명적인 전투 중에 작동 할 수 있도록 합니다.

우리는 정보 영역에서 “상처와 싸울” 수 있어야 합니다. 위기 상황에서 킬 체인을 효과적으로 유지하기 위한 대회에서 승리하지 못하면 치명적인 전투가 발발 할 때 DMO를 수행 할 수 있는 능력이 심각하게 손상됩니다. 이것이 AC2의 핵심입니다 – 장기간의 “정보 차단”을 통해 C2를 수행 할 수 있는 능력입니다. 군대로서 우리는 최악의 경우에 대비해야 합니다. 즉 우리 네트워크가 동 역학적 및 비 키네티적 으로 공격적으로 표적이 되는 치명적인 고급 해상 전투입니다. 전쟁의 잔인한 사실은 해군 네트워크가 명중을 받고 해군이 사상자를 낼 것이라는 것입니다.

현대화 및 혁신 촉진. 우리의 목표는 센서, 무기, 시스템 및 정보를 사용하여 운영 결과를 생성하는 것입니다. 통합 된 연속 캠페인의 일환으로 모든 영역에서 수동적이고 적극적으로 운영합니다. AI / ML 및 기타 기술의 잠재력은 무궁무진하지만 이제 우리의 적들이 이를 어떻게 악용할지에 대해 질문 할 때입니다. 새로운 기술과 시스템이 등장함에 따라 우리는 또한 전쟁 치사율을 개선하기 위해 기존 기술을 창의적으로 사용해야합니다.

이 비전을 통합하여 예상치 못한 문제가 발생할 때마다 언제 어디서나 해결하는 데 필요한 복원력을 달성 하려면 어떻게 해야 합니까? 해군이 요구하는 치사율을 제공하는 데 대한 답은 다음과 같은 능력에 있습니다.

- 민첩하고 적응 적이며 협력 적이어야 합니다.
- 신뢰할 수 있고 지속적인 파트너십 육성
- 정보의 무결성 및 품질 증진
- 네트워크를 효과적으로 보호

마지막으로, 우리는 가장 뛰어난 인재를 모집, 훈련 및 유지해야 합니다. 이것은 이러한 권위주의 정권에 대한 우리의 가장 큰 비대칭 적 이점입니다.

"The Navy is a key partner as the Coast Guard develops and evolves Distributed SIGINT Operations (DSO) as a fully integrated component of Distributed Maritime Operations (DMO). This will require a paradigm shift to a cloud based network that allows cryptologic personnel to directly support Operational and Tactical Commanders from shore based locations and distribute operations to a wide range of SIGINT platforms across multiple Areas of Responsibility. DSO will optimize mission effectiveness and platform capability, taking the Coast Guard from a single cutter operating independently, to a network of multiple cutters, DoD sensors, and overhead assets with round the clock support from operators and analysts ashore."

- Rear Admiral Andrew M. Sugimoto, USCG, Assistant Commandant for Intelligence

페이지 10





Securely operate, maintain, defend, and maneuver Navy networks, communication, and space systems to ensure availability to forces when and where they need it. Networks must be able to fight in a degraded state to achieve warfighting objectives. The caliber of our networks should be our best recruiting and retention tool.

해상 및 해안에 있는 해군 네트워크의 모든 사용자는 공해에서 구축함을 운용하는 것과 동일한 전시 사고 방식을 채택해야합니다. 전시 사고 방식이란 무엇을 의미합니까? 그것은 해군 네트워크의 무결성, 우리 선박의 수밀 무결성에 대해 생각하는 방식에 대해 생각하는 것을 의미합니다. 모든 선원이 기본 피해 통제 자격을 갖춘 것처럼 모든 선원, 민간인 및 계약자는 기본 사이버 보안 자격을 갖추어야합니다. 모든 선원은 X-ray, Yoke 및 Zebra와 같은 선박의 방수 무결성을 설정하는 세 가지 기본 준비 상태를 알고 있습니다. 적절한 재료 조건을 설정하면 사상 자나 적의 공격으로 인한 피해 확산이 느려지거나 방지됩니다. 그것은 함선이 타격을 받아 계속 싸울 수 있게 합니다. 네트워크 복원력에 대한 우리의 정신은 선상 DC의 정신과 같아야 합니다. 네트워크가 타격을 입으면 우리 팀은 신속하게 피해를 평가하고 원인을 파악하고, 피해를 격리하고, 수리하고, 계속해서 싸우고 있습니다. 우리는 지휘관이 방어 사이버 공간 작전을 실행하기 위해 지역 수비수 교육을 통해 네트워크를 조작 할 수 있도록해야합니다.

배의 지휘관은 전투에 들어가기 전에 항상 배에 있는 다양한 시스템의 상태를 알아야합니다. 주 엔진의 상태는 어떻습니까? 모든 사격 통제 레이더가 작동합니까? 그것이 지휘관의 전투 플랫폼에 대한 상황 인식의 핵심입니다.

비교 가능하고 정확한 사이버 상황 인식은 지휘관에게 전투에서 의존 할 수 있는 네트워크의 표현을 제공합니다. 모든 전술 및 작전 지휘관은 자신의 네트워크를 알고, 그들에게 가해지는 위협을 이해하고, 그들이 받아들이고 있는 위험을 인식해야합니다. 이것은 명령 중심의 사이버 작전입니다. 지휘관은 네트워크 무결성을 보장하기 위해 강화 된 예방 조치를 취해야한다고 판단하는 경우 항상 CPCON (사이버 보호 조건) 수준을 높일 권리가 있습니다. 이러한 이유로 해군의 지도부는 사이버 인식 및 사이버 보안을 "사령관의 사업"으로 지정하고 훈련 된 승무원과 임무 준비 장비를 보장하기 위해 개인적인 책임과 책임을 할당했습니다.

데크 플레이트 수준에서 부서, 부서 및 승무원은 시스템에 대한 인식을 개발하고 유지해야합니다. 예를 들어 엔지니어는 주 엔진 및 관련 보조 시스템에 대해 잘 알고 있어야합니다. 이러한 인식은 이러한 시스템의 일상적인 작업과 일상적인 유지 관리에서 비롯됩니다. 상세하고 상황 인식은 무언가가 "정확하지 않은"경우 즉시 인식 할 수 있는 능력을 제공합니다. 이러한 친숙 함 덕분에 숙련 된 감시 팀은 신속하게 행동하고 피해를 완화하여 지휘관이 배와 계속해서 전투를 벌일 수 있습니다. 우리는 해군의 네트워크 전쟁 플랫폼을 안전하게 운영, 유지, 방어 및 조종하기위한 기본 전제 조건이므로 이러한 수준의 사이버 상황 인식 및

핵심 역량을 생성해야합니다.

페이지 11



전략적 이니셔티브 1.1. 해군 전체에 사이버 상황 인식 구축

사이버 상황 인식은 해군 네트워크를 안전하게 운영, 유지, 방어 및 조종하기 위한 중요한 전제 조건입니다. 우리는 사이버 공간 공통 운영 상황을 이해하고 공유하는 능력을 가속화해야합니다. 사이버 건강은 강인함과 탄력성을 의미합니다. 사이버 상태는 성능, 보안 및 취약성을 설명합니다. 지휘관의 전투 네트워크는 데이터, 센서, 전투 시스템 및 플랫폼입니다. 결과는 실행 가능한 사이버 상황 인식이므로 네트워크 운영자와 해군 지휘관은 네트워크에 대한 적의 공격에 맞서 싸우고 방어하며 승리하는 데 필요한 결정을 신속하게 내릴 수 있습니다. 가상화 도구, 데이터 과학, AI 및 교육에 대한 요구 사항을 통해 이 이니셔티브를 추진하여 사이버 준비 상태 대시 보드 및 대응 조치를 알리고 향상시킬 것입니다.

CCORI (Command Cyber Operational Readiness Inspections)는 규정 준수 관점에서뿐만 아니라 임무 평가 및 위협 애뮬레이션을 사용하여 작전 준비 상태와 위험을 평가하여 시스템이 안전한지 확인하는 해군의 수단이 될 것입니다. 이는 네트워크를 넘어서 취약성에 대한 이해를 넓히고 새로운 평가 영역과 기술을 포함합니다.

전략적 이니셔티브 1.2. 탄력적이고 확실한 명령 및 제어 제공

탄력적이고 확실한 C2는 사이버 공간에서 효율적이고 매우 효과적인 자동화 된 기동 수단을 제공하는 프로세스가되어야합니다. 이러한 조작은 물리적 도메인 전체에서 동기화되고, 충돌을 제거하고, 우선 순위가 지정되고, 통합됩니다. 최종 국가는 평시와 전투 중에 선점자 우위를 확보하여 적보다 작전 우위를 확보해야합니다.

탄력적 인 C2를 달성하기 위해 우리는 모든 해군 네트워크의 C2를 보장하기 위해 DODIN-N (Department of Defense Information Network – Navy) 작전을 보호하고 방어하기 위해 사이버 보안 및 사이버 공간 작전에 완전히 참여할 것입니다. 경쟁 스펙트럼 전반에 걸쳐 탄력적 인 C2를 보장하기 위해 우리는 마치 우리가 이미 치명적 전투에 있는 것처럼 경쟁하고 열악한 환경에서 싸우고 기동 할 수 있도록 해군 사이버 부대를 개발하고 훈련해야합니다. 우리는 전투의 위기에 대비하기 위해 지금 사이버 공간에서 기동을 미리 계획하고, 테스트하고, 실행해야합니다. 이를 위해서는 방어 적 사이버 공간 운영 (DCO) (대응 조치, 자동화

된 네트워크 조작 및 장애 조치 옵션)을 포함하지만 이에 국한되지 않는 사전 계획된 대응을 개발해야합니다.

전략적 이니셔티브 1.3. 침입 공격 표면 감소

네트워크와 효과적으로 싸우고 방어하기 위해 해군 네트워크를 엔터프라이즈 네트워크로 통합하는 조치를 시작할 것입니다. 이 엔터프라이즈 네트워크 전환에는 인프라 풋 프린트 감소 및 고급 가상화 기술 구현이 포함됩니다. 또한 자동화 된 사이버 방어 기능을 완전히 활용하여 취약성 관리 프로세스를 최적화 할 것입니다.

경계 보호를 통합하고, 회로 아키텍처를 리팩터링하고, 미션 세트, 클라우드 서비스 및 새로운 네트워크 서비스의 진입로에 집중해야합니다. 클라우드 서비스, 항공기 (유인 및 무인)와 같은 새로운 평가 영역을 포함하도록 검사 프로세스를 확장 할 것입니다. 우리는 네트워크가 본질적으로 적대적이라는 가정하에 "제로 트러스트"모델을 사용하여 운영 할 것이며 사용자와 장치가 자신의 신원을 증명하고 임무 시스템에 액세스 할 수 있어야합니다. 제로 트러스트는 패러다임 전환을 필요로 하며 효과적인 정보 보안 및 복원력 관행을 구현하지 않으면 달성을 할 수 없습니다.

전략적 이니셔티브 1.4. 방어 발전 및 강화

AI / ML 기술을 사용하여 사이버 공간 방어 능력의 모니터링, 감지 및 시각화를 자동화 할 것입니다. 또한 새로운 소프트웨어 정의 네트워크 아키텍처에 대한 대체 라우팅을 자동화하고 "대역 외"관리 네트워크 환경을 구축 할 것입니다. 이 환경은 모든 C2 및 운영 트래픽, 관리, 유지 관리 및 프로비저닝 활동을 전송하기 위한 안전하고 격리 된 통신 경로를 제공합니다. 공격 감지 및 취약성 관리를 개선하기 위해 인텔리전스 및 운영 분석가에게 이러한 기술을 사용하고 네트워크를 더 잘 방어하도록 교육 할 것입니다.

전략적 이니셔티브 1.5. Fleet MOC-to-MOC 통합 및 기동을 통해 C2 향상 및 보장

탄력적이고 확실한 C2는 해군 네트워크를 통해 분산 된 모바일 및 비 모바일 장치를 연결하는 데 중요한 구성 요소입니다. 이러한 유닛 간의 연결을 유지하려면 특히 열악한 통신 환경에서 평시 또는 에스컬레이션 중에 해군 네트워크를 조작 할 수 있는 탄력적인 네트워킹 기술 및 관행이 필요합니다. Fleet Maritime Operations Center (MOC)에 완전히 탄력적인 C2를 통합하기 위해 Fleet MOC의 사이버 부대를 훈련시켜 기동 네트워크를 촉진하고 연습 할 것입니다. 또한 모든 주요 해군 훈련 및 MOC 인증 중에 MOC 대 MOC 사이버 공간 작전 전술, 기술 및 절차를 강조 할 것입니다.

전략적 이니셔티브 1.6. 해군 인수 / PPBE 프로세스에 참여하여 새로운 기능 통합 가속화

우리는 해군 계획의 일환으로 함대 파트너인 해군 정보 부대 (NAVIFOR) 및 해군 작전 책임자 (OPNAV) 해군 작전 담당 부국장 (DCNO)과 긴밀하게 협력 할 것입니다 (N2 / N6). 운영 요구 사항 식별을 가속화하기 위한 PPBE (Programming, Budgeting and Execution) 프로세스. 우리는 인간 데이터 수집 및 분석을 강화하기 위해 데이터 과학, 자동화 및 인공 지능 기능을 강화해야합니다.

페이지 12





향후 5년 동안 해군 암호 전쟁 (CW) 및 CW 엔터프라이즈의 초점은 다음과 같습니다.

- 해상 우월성을 유지하기 위해 우리의 힘과 능력을 발전시키고 장기 전략 경쟁자에 비해 전쟁 우위를 확보하십시오.
- Distributed Maritime Operations (DMO)의 완전히 통합된 구성 요소로서 Distributed SIGINT Operations (DSO)를 발전시킵니다.
- 전투 정신과 전략적 경쟁자보다 훨씬 뛰어난 전문 기술을 갖춘 고도로 동기 부여되고 잘 훈련된 선원의 힘을 유지하십시오.
- 정밀, 장거리, 치명적인 화재를 지원하는 함대 및 합동 사령관 암호 및 사이버 공간 기능을 제공합니다.
- 우리가 원활하게 운영하고 필요할 때 하나의 팀으로 싸울 수 있도록 파트너십 (국가, 합동, 동맹 및 파트너 국가)을 강화하고 확장합니다.

함대 암호 전쟁의 범위

Fleet Cryptologic Warfare 작전은 신호 정보 (SIGINT)를 포함합니다. 전자전 (EW); 사이버 공간 운영 (CO); 스펙트럼 인식 및 전자기 기동 전쟁 (EMW); 신호 보안 (SIGSEC) 및 운영 보안 (OPSEC) 정보 작업 (IO); 정보 관련 능력 (IRC); 방어 적 사이버 공간 운영 (DCO)에 대한 SIGINT 지원.

SCOPE OF FLEET CRYPTOLOGIC WARFARE

Fleet Cryptologic Warfare operations encompass signals intelligence (SIGINT); electronic warfare (EW); cyberspace operations (CO); spectrum awareness and electromagnetic maneuver warfare (EMW); signals security (SIGSEC) and operations security (OPSEC); information operations (IO); information related capabilities (IRC); and SIGINT support to Defensive Cyberspace Operations (DCO).

해상 통제권의 복귀와 전략적 경쟁자에 대한 블루 위터 전쟁의 전망은 함대 수준의 전쟁과 해상에서의 암호 전쟁 (CW)의 주요 역할에 다시 초점을 맞췄습니다. 우리의 CW 부대는 적의 능력, 행동 및 의도를 포함하여 적에 대한 시간 결정적인 전술 및 작전 정보를 지속적으로 제공해야 합니다. DMO의 통합 구성 요소로 작동하는 분산 SIGINT 엔터프라이즈의 일부로 사용 가능한 모든 SIGINT 기능, 정보 소스 및 파트너십을 활용할 것입니다.

우리는 적의 작전 패턴과 기술적 능력을 그 어느 때보다 잘 알고 있어야 하며, 전투 우위를 보장하기 위해 지속적으로 정보를 제공해야 합니다. 글로벌 운영 및 전력 문제가 증가함에 따라 인텔리전스 커뮤니티 (IC), 특히 국가 안보국 / 중앙 보안 서비스 (NSA / CSS)와의 파트너십이 그 어느 때보다 중요해졌습니다. 냉전의 마지막 10년 동안 우리의 CW 성공은 주로 우리의 주요 해양 위협인 전 세계에 배치된 소련 해군에 대한 깊은 작전 및 기술 지식 덕분이었습니다. 우리는 그 시대의 성공에서 많은 것을 배울 수 있습니다.

우리는 국가 및 해군의 임무를 적극적으로 수행하고 이러한 파트너십을 활용하여 함대 사령관이 필요할 때 필요한 정보를 지속적으로 확보하도록 할 것입니다. 우리는 TACSIT에 정보를 제공하고, C5ISRT (지휘 및 통제, 통신, 컴퓨터, 사이버, 정보, 감시, 정찰 및 표적) 도전에서 승리하고 정밀 장거리 공격을 가능하게 하는데 필요한 전투 능력을 제공합니다. 우리는 긴급하게 이러한 중요한 기능을 계속 발전시키고 정상화 할 것입니다.

전략적 이니셔티브 2.1. DMO (Distributed Maritime Operations)의 통합 구성 요소로서 Distributed SIGINT Operations (DSO)지지 및 실행

우리는 모바일 및 비 모바일 DSO 세력이 하나의 긴밀하게 통합 된 팀으로 작동하는 DMO의 완전히 통합 된 구성 요소로 DSO를 계속 발전시킬 것입니다. DSO의 기반은 해군의 즉각적인 정보 요구를 충족하기 위해 사용 가능한 모든 센서, 정보 소스, 분석 기능 및 파트너십을 활용하는 운영 문화에 중점을 둡니다. 여기에는 모든 해상 적들에 대한 적시에 정확한 전술 정보를 유지하고 정밀한 장거리 치명적인 화재를 지원하는 것이 포함됩니다.

이 이니셔티브의 일환으로 Fleet, 국가 및 동맹 파트너와 협력하여 운영 및 기술 변화의 속도로 대응하는 Fleet 암호화 및 EW 기능을 다루는 조치를 추진할 것입니다. 우리는 파트너와 긴밀히 협력하여 연결이 거부되거나 저하 된 기간 동안 미션 연속성을 제공하는 절차를 개발, 훈련 및 실행합니다. 여기에는 DSO에 예비군을 통합하여 모바일 및 비 모바일 서지 옵션을 준비하는 것이 포함됩니다.

DSO 구성 및 관련 작전 문화를 성숙시키는 과정에서 우리는 진화하는 DMO 전쟁 개념과 완전히 일치하여 장기적인 전략적 경쟁의 증가하는 요구를 지원할 수 있는 위치를 확보 할 것입니다. DSO는 또한 함대 사령관의 우선 순위 정보 요구에 부합하는 위임 된 국가 책임의 실행을 지원하고 직접 지원할 것입니다.

전략적 이니셔티브 2.2. 고급 운영 지식, 기술 기술 및 전쟁 문화로 CW 부대를 고취하고 유지하십시오.

우리는 신호 정보, 사이버 공간 작전 및 전자전에서 해군의 탁월한 전문가입니다. 이것이 우리의 학문입니다. 해군의 IW 커뮤니티에 있는 팀원들과 함께 SCC (Service Cryptologic Component) 책임에 부합하여 우리는 CW 부대가 적보다 더 잘 훈련되고, 준비되고, 준비되도록 조치를 취할 것입니다. 현대 훈련, 멘토링 및 리더십의 연속을 통해 전체 경력에 걸쳐 강화 된 첫날부터 우리 국민에게 전쟁 정신을 심어 줘야합니다.

빠르게 발전하는 정보화 시대의 도전과 기회에 직면하고 있으며, 우리의 강력한 적들이 제시하는 도전으로 인해 복잡 해짐에 따라 CW 전문가가 전투에 가져 오는 기술과 지식에 대한 필요성이 그 어느 때보다 커졌습니다. 오늘날의 선원은 데이터가 풍부한 환경에서 자랐으며 정보에 깊이 있고 질문하고 가정에 도전하며 정보 환경을 활용하는 방법을 알고 있습니다. 이 이니셔티브의 책임을 다하려면 CW 커뮤니티의 모든 구성원의 혁신이 필요합니다. 이 약속에는 SIGINT 정보를 얻고, 알고, 사용하는 방법에 최고가되는 것이 포함됩니다. 첫날부터 기술적인 통찰력과 전문적인 기술을 발전시키는 데 완전히 참여합니다. 모든 해군 전쟁 지역에 정보를 신속하게 적용하는 방법을 알고 있습니다.

전략적 이니셔티브 2.3. 적의 운영 및 의도에 대한 심층 분석을 수행하고 제공하여 전쟁 우위를 창출합니다.

해상 우월성을 유지하는 데 있어 성공의 열쇠는 의도를 알기 위해 잠재적인 적을 더 깊이 이해하는 것입니다. 우리는 장기 전략 우선 순위에 중점을 두고 장기 분석 핵심 역량을 발전시킴으로써 이러한 깊이 있는 지식을 구축 할 것입니다. 여기에는 일부 힘 재정렬과 더 중요한 것은 클라우드 컴퓨팅, AI / ML 및 인간 언어 기술 (HLT)과 같은 고급 정보 관리 및 분석 기능의 현명한 사용을 포함하는 조정 된 조치가 포함됩니다. 또한 이러한 심층적인 이해를 보안 인증 및 평가 프로세스에 통합하여 예상되는 적대적 위협으로부터 네트워크와 시스템을 강화할 것입니다.

우리는 또한 국가, 공동 및 동맹 파트너와의 긴밀한 운영 파트너십을 통해 이 이니셔티브를 달성 할 것입니다. 우리의 잠재적인 적들에 대한 더 깊은 이해를 얻음으로써, 우리는 기동, 화재 및 대응 조치를 지원하기 위해 지원되는 함대 지휘관에게 정보를 제공하는 데 더 중요한 역할을 할 것입니다.

전략적 이니셔티브 2.4. 시기 적절하고 반응이 빠른 기술 신호 분석을 통해 전투 능력 향상

소는 큰 키를 드리겠습니다 전에는 TACOM을 달았으나 키에 드리겠습니다 액정에는 정답에 대한 키의 지식과 마찬가지로 기술 및 기능적으로 계속해서 진화하고 있습니다. 우리는 기술 신호 분석을 수행하여 우리 함대를 위협하는 전투 능력에 대한 최신 지식을 확보하고 자체 전투 및 무기 시스템이 변화 속도에 따라 "재 장전" 기능을 제공하는 프로세스를 통해 이러한 위협을 감지하고 물리 칠 수 있도록 지원할 것입니다. 이것은 전자기 스펙트럼 (EMS)을 더 잘 이해하고 조작하는 데 중요합니다. 오늘날의 위협 환경의 복잡성과 기술의 속도로 인해 우리는 지식과 분석 능력에 대한 기술적 깊이를 신속하게 적응하고 개발할 수 있는 능력을 발전시켜야 합니다.

우리는 우리 능력의 상호 운용성과 전체 데이터 및 정보 공유를 보장하기 위해 국가 및 공동 파트너와 긴밀히 조정하고 조정하여 이를 수행 할 것입니다. IC 및 DoD 전반에 걸쳐 Technical SIGINT (TechSIGINT)의 활성화를 수용하여 적의 전투 시스템의 기술적 측면과 관련 전술, 기술 및 절차 (TTP)에 대한 자세한 지식을 개발할 것입니다. 함대가 필요로 하는 전투 능력을 지속적으로 확보 할 수 있도록 기술 정보를 제공하는 것이 필수적입니다.

전략적 이니셔티브 2.5. 향상된 상호 운용성, 공유 기능 및 신속한 정보 교환을 통해 국가, 합동, 연합 및 파트너 관계 강화

해양 우월성을 유지하는 데 있어 작전 파트너십의 중요성은 아무리 강조해도 지나치지 않습니다. 이는 특히 CW 작전의 경우 고급 해상 전에서 CW 작전의 전체 범위를 실행하기 위해 전문 지식, 센서 및 능력에 점점 더 의존 할 것이기 때문에 특히 그렇습니다.

고급 신호 환경에서 운영하고 전투 이점을 위해 국가 및 전술 정보 액세스의 균형을 효과적으로 조정하는데 있어 우리의 성공은 우리가 보유한 모든 파트너십에 달려 있습니다. 해군의 서비스 암호화 구성 요소로서 우리는 암호화 및 EW 시스템과 기능이 완전히 상호 운용되고 SIGINT 기업 전체에서 원활하게 정보를 공유하도록 함으로써 파트너십을 구축하고 강화할 수 있는 모든 기회를 추구 할 것입니다.

페이지 14



Expand on our ability to deliver warfighting effects (movement, maneuver, and fires) through cyberspace that enables naval commanders to fully employ their forces in support of Distributed Maritime Operations (DMO).

사이버 공간뿐만 아니라 전투 능력과 효과를 제공하는 것이 함대 수준의 전쟁의 진화에서 이 사령부의 주요 책임입니다. 이러한 기능을 계획, 개발 및 실행하는 우리의 능력은 적의 능력과 우리를 아는 능력을 약화시킵니다. 우리의 능력은 우리의 C2를 최우선으로 방어하고 사이버 공간, 우주 및 전자기 스펙트럼을 통해 명백히 강력한 힘을 가져 오기 위해 움직임, 기동 및 화재를 제공해야 합니다. 우리는 미국 사이버 사령부의 지속적인 참여 및 전진 방어라는 전략적 개념과 함께 목표를 달성 할 것입니다. 이러한 개념은 우리 선원들에게 친숙해야 합니다. 무력 충돌이 없는 적의 캠페인에 지속적으로 경쟁하고 좌절시키는 꾸준하고 지속적인 활동입니다. 해군은 전진 방어의 오랜 역사를 가지고 있습니다.

해군, 해병대 및 해안 경비대는 특히 사이버 공간을 통해 전투 능력과 효과를 제공하는 것과 동일한 철학을 가져야합니다. 특히 사이버 공간을 통해 우리는 적의 사이버 공간에서 방어 조치를 취하여 공격 계획을 좌절시키고 공격 효과를 제공하여 그들을 물리칠 수 있습니다.

전략적 이니셔티브 3.1. 해양 운영 센터 (MOC)에서 IW C 기능 및 효과의 운영 고용 및 동기화를 가속화합니다.

Fleet MOC에서 IW 기능 및 효과 전달을 통합하고 동기화하는 기능은 DMO 실행의 핵심 인 전쟁의 필수 요소입니다. IW 기능과 정보 소스의 통합은 MOC가 모든 적의 위치와 의도에 대해 일관된 실시간 BA를 유지하는 데 핵심적인 역할을하여 유리한 TACSIT가 유지되고 있는지 여부와 상관없이 장거리 치명적인 화재를 지시합니다. 운동 또는 비 운동.

TENTH Fleet의 MOC 및 작전 부대는 국가 및 작전 ISR의 통합을 촉진하고 자원을 목표로하여 BA를 강화 할 수 있는 위치에 있습니다. 우리는 이를 중심으로 C10F MOC 작전을 발전시키고 미국 사이버 및 우주 사령부의 해군 구성 사령관과 국가 안보국의 서비스 암호화 구성 요소로서의 책임과 권한을 통합하여 DMO 이점을 더욱 창출 할 것입니다. Fleet MOC 파트너와 협력하여 MOC-MOC 프로세스를 구현하고 IW 기능을 OLW (Operation Level of War) 계획에 보다 원활하게 적용하고 신뢰할 수 있고 시기 적절한 정보 공유를 가능하게 하는 데 필요한 인프라를 개발할 것입니다.

15 페이지



전략적 이니셔티브 3.2. 사이버 효과를 신흥 해군 및 해병대 전쟁 개념에 통합하기

해군 부는 해군과 해병대의 긴밀한 통합을 통해 해상에서의 주요 분쟁에서 승리 할 것을 약속합니다. 이를 위해 해군과 해병대는 DMO, LOCE (Littoral Operations in a Contested Environment) 및 EAEO (Expeditionary Advanced Based Operations)와 같은 혁신적인 개념을 개발하고 있습니다.

그더는 애정내외 신분인 협약을 통해 이니티브 신설에 따른 신경 / 기금 확장과 함께 협약을 체결하는 것을 포함합니다. 여기에는 이러한 개념에 따라 IW 기능이 군대 기동에 기여하는 것도 포함됩니다. 여기에는 전쟁 게임, 실험 및 연습에서 방어 및 공격 사이버 효과를 제공하기 위한 혁신적인 우주 및 해양 기반 접근 방식을 탐색하는 것이 포함됩니다.

전략적 이니셔티브 3.3. 합대 및 합동 작전 전반에 걸쳐 사이버 공간 효과의 개발, 계획 및 전달을 촉진하고 발전시킵니다.

우리는 동맹국과 파트너의 적극적인 지원으로 싸우고 승리 할 것입니다. 모든 파트너와 협력하여 사이버 공간 효과의 개발, 계획 및 전달을 촉진하고 발전시킬 것입니다. USCYBERCOM과 긴밀히 협력하여 주요 전쟁 시나리오에서 사이버 효과를 전달하는 데 특히 도움이되는 지원 및 기여를 가진 파트너를 식별 할 것입니다.

우리는 소규모 전술 사이버 팀의 작전 고용을 포함하여 합대 수준의 전쟁 및 DMO를 지원하는 혁신적인 접근 방식 개발을 주도 할 것입니다. 여기에는 합대 작전을 직접 지원하는 전술 단위의 지속적인 발전을 주도 할 작전 요구 사항의 식별, 검증 및 홍보가 포함됩니다.

우리는 사이버 공간 효과 및 화재 전달을 통합하기 위해 합대 전체에 전문성과 지원을 제공하기 위해 C10F MOC에서 고급 전투 "해상 화재 셀"을 개발할 것입니다. 우리는 사이버 효과에 대한 새로운 교리의 개선과 성숙을 알리고 구체화하고, 그러한 교리의 다음 세대를 가져올 실험과 혁신을 계속 추구 할 것입니다.



16 페이지





Grow the capacity and capability of the Navy's cyber teams to meet the demands of Persistent Engagement and Defend Forward. As we evolve the Nation's cyber mission force, we will develop the requirements for Fleet cyber operations teams servicing naval targets.

2015-2020 전략 계획이 발표된 이후, 우리는 원래 목표의 주요 목적을 달성하기 위해 운영중인 사이버 미션 팀을 구성했습니다. 우리는 공동 전쟁 요건을 충족 할 수 있도록 사이버 부대의 능력과 능력을 지속적으로 평가합니다. 앞으로 우리는 해양 우위를 확보하고 DMO를 실현하는 데 필요한 사이버 힘과 역량을 추구 할 것입니다.

전략적 이니셔티브 4.1. 운영 요구 사항을 통해 힘 생성 및 기능 요구 사항 추진

해군 작전 책임자 (CNO)는 Fleet를 위한 유기적 전술 사이버 팀의 개발 및 배치에서 NAVIFOR를 지원하도록 FCC에 지시했습니다. 우리는 NAVIFOR 및 해군 정보 전쟁 개발 센터 (NIWDC)와 협력하여 요구 사항, TTP 및 기능을 설정해야 합니다.

이 사령부는 Fleet IW 시스템 및 인프라에 대한 기능 향상 및 업그레이드를 추진하는 운영 요구 사항을 개발, 검증 및 홍보하는 운영 책임자입니다. 여기에는 NCWDG (Navy Cyber Warfare Development Group) 와 협력하여 새로운 사이버 기능 및 도구 개발이 포함되지만 이에 국한되지는 않습니다. 우리는 최첨단 IW, EMS 및 사이버 전투 능력의 개발과 제공을 보장하기 위해 IW 커뮤니티의 요구 사항과 우선 순위를 형성하는 데 주도적 인 영향력을 발휘해야 합니다.

전략적 이니셔티브 4.2. 성숙한 조직 구조, 관계 및 명령 및 통제

우리는 합동 군 본부 – DoDIN (JFHQ-DoDIN), 합동 군 본부 – 사이버 (JFHQ-C), 태스크 포스 태평양 (TF-P) 간의 조직 관계, 구조 및 C2 관계를 지속적이고 엄격하게 실행, 평가 및 필요한 경우 수정해야 합니다.), 태스크 포스 사우스 (TF-S), 사이버 작전 – 통합 계획 요소 (COIPE), 합동 MOC (JMOC), 해군 사이버 부대 및 역량을 향상시키는 데 활용할 수 있는 다른 파트너십을 모색합니다.



Maintain maritime superiority from the sea floor to space with a core emphasis on lethality, readiness and capacity. With the re-establishment of U.S. Space Command and creation of U.S. Space Force, we must re-focus to provide comprehensive space capabilities to support all domain operations.

해군은 60년 이상 우주에 의존해 왔습니다. 1958년 해군 연구소는 최초의 인공 위성 중 하나를 발사했습니다. 1970년대에 해군은 해상 통신용 위성을 개발했으며, 1980년에 공동으로 인수한 함대 위성 통신 시스템은 해군의 전술 및 장거리 지휘 및 물류 지원 통신에 보편적으로 사용되었으며 결국 모든 서비스에 채택되었습니다. 1990년대에 우리는 해군이 할당한 위성 군을 운영하기 위해 Naval Satellite Operations Center (NAVSOC)를 설립했습니다. 오늘날 우주는 해군 작전의 원활한 부분이며 해군은 통신, 항법, 감시, 날씨 및 해양 지원을 위해 우주에서 가장 의존하는 서비스입니다.

우주에서의 도전은 우리가 사이버 공간에서 직면하는 것만큼이나 현실적입니다. 우리의 전략적 경쟁자들은 우주에 대한 우리의 의존도를 이해하고 활용하기를 희망합니다. 그들은 강력한 우주 기반 인텔리전스, 감시 및 정찰 (ISR) 기능을 개발했습니다. 그들은 궤도 및 지상 기반의 재밍 기능, 지향성 에너지 무기 및 대위성 (ASAT) 시스템을 개발하고 있습니다. 우리의 장기적인 전략적 경쟁에 대한 우주의 중요한 관계는 미 우주 사령부를 재건하고 미 우주군을 설립하기로 결정한 원동력이었습니다.

해군 우주 사령부 (NAVSPACECOM)로서 오늘날 우리는 해군의 할당된 위성 시스템, 지상국 및 네트워크에 대한 작전을 조직하는 동시에 DMO에 대한 우주 상황 인식을 통합하고 해군 임무를 지원하기 위한 우주 제어 기능을 제공합니다. 미국 우주군이 성숙함에 따라 우리는 해군의 우주 요구 사항을 계속 옹호하고 함께 전체 우주 작전 계획 전문 지식을 제공해야 합니다. 우리는 이러한 중요한 자산의 보안을 보장할 수 있도록 준비해야 합니다.

전략적 이니셔티브 5.1. 우주 및 해양 전략 통합

우리는 함대를 통합하고 이익을 얻기 위해 USSPACECOM과 긴밀한 관계를 맺어야 합니다. 이 관계를 조성하기 위해 사이버 사령부는 USSPACECOM과 협력하여 우주 및 해양 전략을 통합하는 협력을 확장합니다. 이를 통해 우리는 우주 및 해양 전략을 통합하여 전략적 이니셔티브 5.1. 우주 및 해양 전략 통합을 실현합니다.

이 시기에는 신성한 진리를 그려, 삶의 향기를 찾는 드림커뮤니티에 대한 관심과 함께, 미래의 해군 전투에 대한 중요성을 명확히 할 수 있어야 합니다. 우리는 작업 및 공간 능력의 상태에 대한 동기화 및 공유 상황 인식을 보장 할 연락 담당자 (LNO) 위치를 설정할 것입니다.

페이지 18



전략적 이니셔티브 5.2. 미 우주군과 미 우주 사령부에 대한 해군 요구 사항을 대표

새로운 USSPACECOM의 해군 구성 요소로서 우리는 USSPACECOM에 제출할 때 해군의 공간 요구 사항과 능력 격차가 정확하고 최신 상태인지 확인해야 합니다. 이를 위해서는 미국 우주군 및 USSPACECOM과의 관계를 활용해야 합니다. 또한 해군 작전 총장실 (OPNAV)과 해군 공간 요구 사항을 조정하기 위해 해군의 프로그래밍 프로세스에 대한 지식과 함대 사령부의 DMO 전쟁 교리의 지속적인 개발에 대한 중요성이 필요합니다.

전략적 이니셔티브 5.3. 이동과 기동의 자유를 보장하기 위한 우주전 기술 개발 및 개선

우리는 큰 권력 갈등이 해양과 사이버 영역뿐만 아니라 우주 영역에서도 치열한 전투를 포함 할 것이라는 전망에 대비해야 합니다. USSPACECOM이 성숙함에 따라 우주에서 전투 작전을 포함한 작전을 위한 다양한 시스템과 전술을 개발, 개선 및 구현할 것입니다. 우리는 시스템 및 전술에 대한 전문 지식을 개발하기 위해 USSPACECOM과의 관계를 활용하여 기존 및 새로운 우주 기능을 함대 및 공동 작전에 완전히 통합하고 USSPACECOM의 TTP 개발에 알릴 수 있도록해야 합니다.

전략적 이니셔티브 5.4. 통합 된 해군 공간 관점 보장

우리는 해병대와 협력하여 통합에 경쟁과 갈등의 연속체에서 우주 작전의 역할에 대한 적절한 관점이 포함되도록해야 합니다. 우리는 우주 인력, 기술 및 훈련의 개발을 알리기 위해 운영 요구 사항을 연구, 검증 및 홍보 할 것입니다.

전략적 이니셔티브 5.5. 새로운 기술 및 개념 활용

우주가 상용화되고 글로벌 우주 산업이 확장됨에 따라 국제 파트너십이 성장함에 따라 기술 및 비용 장벽이 무너질 것입니다. 상업 우주 부문은 자체 우주 발사, 통신, 우주 상황 인식, 원격 감지, 심지어 인간 우주 비행을 개척하고 있습니다. 이 회사들은 정부에 제품을 공급할뿐만 아니라 상업적으로도 경쟁합니다. 이 영역에서 우리의 우위를 유지하기 위해 우리는 군사적 용용이 가능한 우주에서 잠재적인 상업적 발전을 탐구해야 합니다.



페이지 19



오늘날의 정보 공유는 그 어느 때보다 근본적이고 구조적으로 훨씬 다릅니다. 속도와 민첩성은 성공의 주요 원동력입니다. 이전 프로세스를 더 빠르게 조정하는 것은 작동하지 않습니다. 우리는 끊임없는 변화, 적응 및 혁신에 적합한 새로운 모델을 발명해야 합니다.





따라서 우리는 5년 전 원래의 전략 목표에 대한 근본적인 가정을 재검토하고 일반적으로 타당하다는 것을 알았지만 대 권력 경쟁의 과제를 해결하기 위해 필요에 따라 수정했습니다. 우리는 우리의 주요 전략적 경쟁자들을 능가하기 위해 계속해서 우리의 가정을 재검토 할 것입니다. 우리는 전략적 환경과 적의 의도를 정확하게 이해해야합니다. 고르게 머무르는 것만으로는 충분하지 않습니다. 앞서 나가야합니다.

사이버 보안에서 기술 혁신, 네트워크 방어에서 공격적 사이버 작전 실행에 이르기까지 우리는 동료 및 적을 피어 공격자보다 공격에 대해 더 빠르고 민첩하며 더 효과적이어야합니다. 위기나 갈등이 발생하는 경우, 우리는 장기간의 글로벌, 다중 영역 및 공동이 될 포괄적인 IW 캠페인을 계획하고 준비해야합니다. 이 캠페인은 경쟁과 갈등의 연속성에 걸쳐 진행됩니다.

사이버 공간 영역은 사이버 지속성 전략(지속적인 전술적, 운영적 및 전략적 이점을 생성하기 위해 지속적인 운영 접촉에서 사이버 기능을 사용)과 우리가 선택한 시간과 장소에서 사이버 공간을 통해 그리고 사이버 공간에서 효과를 제공 할 수 있는 능력을 요구합니다.. 먼저 움직여야합니다. 즉, 먼저 결정해야합니다. 우리는 오늘 밤 싸울 사치가 없습니다. 우리는 오늘 싸움에 있습니다.

2020-2025년 전략 계획의 발표는 시작에 불과합니다. 이 계획의 비전을 현실로 만들 일련의 캠페인 및 실행

우리는 이 전략 계획을 개발했습니다. 국가는 그 이하를 기대합니다!

페이지 20

용어 사전

확실한 명령 및 제어 (AC2). 적들이 사용하는 장기간의 "정보 봉쇄"가 있는 상황에서 특히 경쟁이 심하거나 거부 된 작전 조건 하에서 지휘 및 통제를 행사할 수 있는 해군의 능력을 유지합니다. (전략적 계획 2015-2020)

공격 표면. 조직의 보안 위험 노출 합계입니다. 모든 소프트웨어, 하드웨어, 폼웨어 및 네트워크에서 알려진, 알려지지 않은, 잠재적 인 모든 취약성과 제어의 집합체입니다. 공격 표면이 작을수록 조직의 악용 가능성이 낮아 위험이 줄어 듭니다. (전략적 계획 2015-2020)

배틀 스페이스 인식 (BA). 해양 및 정보 전장에 대한 지속적인 감시를 포함합니다. 적의 능력과 의도에 대한 궤뚫는 지식; 적들이 언제, 어디서, 어떻게 작동하는지에 대한 이해 그리고 전자기 스펙트럼 내의 전문 지식. 동기화되면 운동 및 비 운동 모두에 힘을 적용하는 데 필요한 표적 획득 및 표적화 솔루션을 제공합니다. (정보 지배력 달성을 위한 해군 전략 2013 – 2017.)

명령 및 제어 (C2). 임무를 수행하기 위해 할당되고 부착 된 부대에 대해 적절하게 지정된 사령관에 의한 권위와 지시의 행사. (JP 1)

명령 및 제어, 통신, 컴퓨터, 사이버, 정보, 감시, 정찰, 타겟팅 (C5ISR). C4ISR에 "사이버" 및 "타겟팅"을 추가하여 기존 C4ISR에 대한 사이버 공간 도메인의 중요성을 강조하고 일반적으로 무기 시스템의 킬 체인이라고 하는 것에 대한 C4ISR 및 사이버 공간 작전의 수렴 증가에 주목하기 위해 타겟팅하는 해군 용어입니다. 공동 용어에서 킬 체인은 일반적으로 F2T2EA (찾기, 수정, 추적, 목표 지정, 참여 및 평가)라고 합니다.

명령 및 제어 환경. 해군이 직면 할 것으로 예상하는 C2 환경의 범위는 다음과 같습니다. 허용 C2 : 군대를 네트워크화하고 행동의 자유를 가능하게 하는 데 충분한 통신 및 네트워킹 인프라; 이의 제기 된 C2 : 적대 행위가 확대되면 군대가 네트워킹, 위성 통신 (SATCOM) 및 GPS (Global Positioning System) 기능에 대한 위협이 증가하는 환경으로 이어질 수 있습니다. 그러한 위협에도 불구하고 해군은 작전 목적을 위해 적어도 하나의 통신 경로를 유지합니다. 그리고 경쟁이 심한 / 거부 된 C2 : 추가 확대는 적의 행동으로 인해 군대가 상업 및 군사 관련 네트워킹 기능을 거의 완전히 상실하게 되는 경쟁이 치열하거나 거부 된 C2 환경으로 이어질 수 있습니다. 해군은 대부분의 정보 요구 사항에 대해 단 하나의 통신 경로를 제공해야 합니다.

COP (Common Operating Picture). 협업 계획을 용이하게하고 상황 인식을 달성하기 위해 모든 계층을 지원하는 하나 이상의 명령이 공유하는 관련 정보의 동일한 단일 디스플레이. (JP 3-0)

사이버 보안. 보호 된 사이버 공간 내에서 컴퓨터, 전자 통신 시스템 및 기타 정보 기술 (플랫폼 정보 기술 및 그 안에 포함 된 정보 포함)에 대한 무단 액세스, 악용 또는 손상을 방지하여 가용성, 무결성, 인증, 기밀성 및 부인 방지. "사이버 보안" 또는 "사이버 공간 보안"이라고도 합니다. (JP 3-12)

앞으로 방어하십시오. US Cyber Command의 지속적 참여 전략 개념의 핵심 구성 요소입니다. 가장 영토에서도 적에 맞서 작전하여 중요한 군사 및 국익을 방어하는 것을 의미합니다. (커맨드 비전 미국 사이버 사령부)

방어 적 사이버 공간 운영 (DCO). 진행 중이거나 임박한 악의적 인 사이버 공간 활동을 물리 쳐서 블루 사이버 공간 기능을 활용하고 데이터, 네트워크, 사이버 공간 지원 장치 및 기타 지정된 시스템을 보호하는 기

등을 보존하는 임무입니다. (JP 3-12)

국방부 정보 네트워크 (DODIN). 상호 연결이든 독립 실행이든 상관없이 전투원, 정책 입안자 및 지원 담당자에게 필요한 정보를 수집, 처리, 저장, 배포 및 관리하기 위한 정보 기능 및 관련 프로세스 집합입니다. DODIN의 해군 구성 요소를 DODIN-Navy 또는 DODIN-N이라고 합니다. (JP 6-0)

DMO (Distributed Maritime Operations). 먼 거리, 여러 영역에 분산 될 수 있는 전투력의 고용을 통해 해상 통제를 획득하고 유지하는 데 필요한 함대 중심 전투 능력을 최대화하기 위해 통합, 분배 및 기동의 원칙을 결합하는 해군의 전반적 운영 개념, 다양한 플랫폼이 있습니다. (Navy.mil)

분산 신호 인텔리전스 (DSO). OLW (작전 수준) 및 TLW (전술 수준)에서 함대 사령관의 즉각적인 정보 요구를 지원하기 위해 실행되는 통합 모바일 (수상, 항공) 및 비 모바일 (육상) 암호화 작업입니다.

EABO (Expeditionary Advanced Base Operations). LOCE 개념 (아래 참조)과 해군의 DMO를 보완하기 위한 해병대 개념 (2020년 현재 개발 중). 해군 ISR 자산, 미래의 해안 방어 순항 미사일, 대공 미사일 (순항 및 탄도 미사일과 항공기에 대항하기 위한), 전방 무장 및 급유 지점 (FARP) 및 기타 항공기를 위한 원정 작전 기지를 배치하는 데 사용되는 원정 첨단 기지를 구상합니다. 함선 및 잠수함을 위해 팀을 재 장전하거나 주요 해양 지형을 제어하고 해상 통신선 (SLOC) 및 초크 포인트의 보안을 개선하거나 적에 대한 사용을 거부하기 위해 표면 검사 / 정찰 플랫폼에 원정 기지를 제공합니다. 섬 체인에 의해 형성된 자연 장벽은 잠재적인 적에게 "해상 거부 테이블을 돌릴" 기회를 제공합니다.

First Mover Advantage. Wayne Hughes의 Fleet Tactics에서 "효과적인 우선 공격" 개념의 업데이트 된 버전은 특히 사이버 공간 영역 및 전체 스펙트럼 정보 전쟁에서 작전의 시대에 이점이 먼저 이동하는 쪽에 있다는 전술적 철학을 강조합니다.

페이지 21

Great Power Competition (GPC). 용어는 일반적으로 2018년 국방 전략 (NDS, 분류되지 않은 요약)이 국가 안보 전략이 수정 주의적 세력으로 분류하는 "장기, 전략적 경쟁의 재 등장"으로 특징 지어지는 것에 적용됩니다. NDS에 따르면 "중국 및 러시아와의 장기 전략 경쟁은 미 국무부의 최우선 과제이며 오늘날 미국의 안보와 번영에 미치는 위협이 크기 때문에 증가하고 지속적인 투자가 필요합니다. 앞으로 이러한 위협이 증가 할 가능성이 있습니다."

정보 전쟁 (IW). 널리 사용되는 해군 용어는 "적의 정보를 저하, 거부, 기만 또는 파괴하기 위해 해군의 정보 기반 기능 (통신, 네트워크, 정보, 해양학, 기상학, 암호학, 전자전, 사이버 공간 작전 및 우주)을 통합적으로 사용하는 것입니다. 환경 또는 아군 작전의 효율성을 높이기 위해" (NDP-1, Naval Warfare).

통합 화재 (IF). 해군 네트워크, 사이버 공간 및 우주 기능을 사용하여 적의 취약성을 악용하고 공격하여 비 운동 효과 (예: 화재)를 달성합니다. 비 키네티ック 대안이 키네티ック 솔루션과 함께 고려되도록 함으로써 전진 배치 된 해군 사령관을 위한 옵션을 확장합니다. (정보 지배력 달성을 위한 해군 전략 2013 – 2017.)

경쟁 환경에서의 Littoral Operations (LOCE). 해군-해병대 혁신을 위한 통합 프레임 워크를 제공하기 위해 "새로운 위협에 비추어 연안 환경에서의 해군 작전"을 설명하는 해병대 전투 개념 (비밀 및 미분류 버전). 그것은 해상 통제 전투를 지원하기 위해 해상 기반 및 육상 기반 해병대 능력을 사용하는 것을 포함하여 해상 통제를 위한 전투 및 획득에 다시 강조점을 둡니다." (해병대 전투 개발 사령부)

지역 수비수. 사이버 침입 또는 공격에 대응하여 시스템 또는 네트워크를 담당하는 시스템 관리자, ISSM (정보 시스템 보안 관리자) 또는 시스템 보안 분석가의 역할을 맡은 개인을 설명하는 데 사용되는 해군 용어입니다. Local Defender는 관리 권한과 네트워크 / 시스템을 구성하는 요소 및 정보 흐름이 발생하는 방식에 대한 도메인 지식으로 인해 첫 번째 방어선입니다.

해양 운영 센터 (MOC). MOC는 주로 작전 및 전술적 비상 대응 작전을 처리 할 수 있는 지속적인 감독 및 계

획 능력을 제공하고 해상 사령관의 지휘 및 통제하에 할당되거나 할당 된 부대를 관리함으로써 해상 사령관의 기능적 능력을 확장합니다. (FFC / C10F 전략 계획 2015-2020).

지속적인 참여. 미 사이버 사령부의 전략 개념으로의 전환의 핵심 요소는 대응 부대가 아닌 지속력을 중시하는 것입니다. USCYBERCOM이 전 세계적으로 지속적으로 대규모로 적과 경쟁하고 경쟁 할 수 있는 권한을 부여하여 이미 진행중인 전략적 경쟁에보다 효과적으로 참여합니다. (커맨드 비전 미국 사이버 사령부)

기술적 상황 (TACSIT) . 공식적인 해군 용어는 아니지만 세 가지 범주에서 부대의 전술 상황 (TACSIT)을 지칭하는 데 널리 사용됩니다. TACSIT 1 – 배치 및 표적화 된 부대; TACSIT 2 – 알려진 힘 위치; 처리 불명; 및 TACSIT 3 – Forces Not located.

TechSIGINT. 기술 신호 인텔리전스라고도 합니다. 기술적 특성을 결정하는 것은 신호 분석에서 파생 된 가능입니다.

제로 트러스트 모델. 오늘날의 사이버 환경에서는 적들이 이미 우리 네트워크에 있다고 가정하는 것이 더 안전합니다. 따라서 제로 트러스트 모델 프레임 워크는 "신뢰할 수 있는"네트워크 트래픽이 없다고 가정합니다. 신원은 새로운 네트워크 경계입니다. 액세스하려면 신원, 장치, 위치 및 애플리케이션에 대한 엄격하고 반복적인 확인이 필요합니다. 이러한 변수 속성을 기반으로 사용자에게 리소스 및 데이터에 대한 최소 권한 액세스 권한이 자동으로 부여됩니다.





22 페이지





마리오 불 카노

□ 2020년 8월 1일
미분류

" 미국 함대 사이버 사령부 / 미국 10 대 함대 – 전략 계획
2020-2025 " 에 대한 2 개의 생각

1. 제임스 R 킹

2020년 8월 1일 16:06

은퇴 한 것이 기쁘다 – 오늘날 해군에서는 결코 성공하지 못할 것이다. 나는 이것을 읽는 것만으로도 정신적으로 흠뻑 젖었다. 알려 주셔서 감사합니다 //JK

2. 익명

78월 2020 17:03

여기 afloat cryptologic에 관한 모든 것은 단순히 립 서비스입니다.

WORDPRESS.COM 제공 .

위로 ↑