Drone kill net part i.MOV

Sabrina Wallace [00:00:01] I'm good enough to stand on my own. I don't need help. But I can assure you that I have plenty of help if I want it. And I don't. I just want to be able to talk to people about the things mathematically that they're going to want to be taking a look at. And I'm allowed to talk about pretty much anything I want to so long as I stay within the realm of keeping people's very private details out of it. High precision silicon integrated vehicular ad hoc on chip LiDAR on the chip Micro sensor data on the chip. Quasi optical imager. Passive millimeter wave Imager. Geostationary orbit Microwave Phased array for the most up to date one gigahertz 64 channel Cross core relay synthetic aperture radar, which pisses me off any time I try to talk about it. Distributed coherent aperture radar Microwave imaging in microwave emerging radiometer re Digital Beamforming and Imaging Radiometer re Network Engineer. Okay. Now, that is a little preview for things with software defined networking, etc., that I may or may not go back into depending on how people behave. Frequency generators versus true life machines. Nine years ago. I liked the way this gentleman spoke and I told the synergies I would be back with this.

Speaker 2 [00:01:37] Explication. Usually not not this thing like the regular bob back one. I used to do a lot of hours. I've been using it for years. They want to use it. Ruler of ours. I got more energy. But when you start out doing these things, what happens is. Well, what's the latest with that? It's just not a right machine. If you had it right. Yeah, like real life knowledge, man. You conquer the world, but don't put out the medical establishment out of business, you know? Yeah, Believe me, the average professional doctor is in business for business. And, yeah, a lot of women say we say, you know, marry doctors. They, like, married. You know, their mother told them, go marry a doctor, You make a lot of money. So you guys are under pressure. You know, if he saw a machine, they could put him out of business. I mean, you don't even have to be the medical staff. So it can be just the average professionals out there. They. You know what? They wouldn't like it. They wouldn't like it at all. I know they would even cure people who are so busy it would just cut them out of business all the way.

Sabrina Wallace [00:02:52] So just keep that in mind in regards to more than just your race machine. As we continue to plug along here through all these different articles in all of these different places. So near body Electric Field effect. Fiber channel over Ethernet. So when we're using fabric networks back and forth, mesh, star mesh hybrid, whatever, we just translate the data in the ubiquitous storage or not software defined networking and toss electrical signals back and forth and route the data back over the Ethernet or the fiber. Okay. So now I am going to show you software defined networking use case end to end quality of service. Now, normally I don't take people to blogs, but this is about Cisco Systems and we're talking about the control plane, a data center, a wide area network, or a service provider. Utilizing APIs means people using software on their phone, API on campus. This is end to end quality of service for a drone kill strike type of scenario and how we shut off networks. Heterogeneous software defined networking case scenario. And this is a use case scenario. Correct. Billing adequate bandwidth policy enforcement supported routing protocol, IP address assignment, Internet Gateway found whether or not we're able to grant or restrict access based on policy, ability to assign IP address, dynamically controller, replace existing route protocols with your man net, which could have a radio data link network connected to it. And so while I was looking through all of that, I went ahead and bounced into the Borg control plane orchestration and details on our software defined networking end to end with all this. And that sounds interesting. So this post is in some ways an extension where he's talking about quality of service in a converged environment. As I explained about the mesh networking voice over IP or both. This will be a good example of a case where software defined networking very efficiently solves a policy problem. Policy is about how we route the size of the bandwidth and where we allocate where we are going to put up with broadcast storms. You're welcome. Again, that is presented and unfortunately not large number of networks today. For many organizations, large or small, the network is approached with a very siloed, good enough mentality, meaning that each portion of an organization's technology implementation is typically allocated to those that have particular skill set. The folks that configure and maintain the data center network can often be a separate group, or at least a separate person come from the folks that support the campus network infrastructure, which is even further removed from the team that manages the server infrastructure, the storage infrastructure, all of which have a piece to play in what should be considered the organization's global mobile information grid for wind yet again global quality of service policy. But it is a generic networking term global obviously, of course, in

small to medium environments, many of these roles are consolidated down to a few folks, but even then there are silos and where there are silos, communication tends to be more difficult. So the control playing on the Cisco back end, do you want to police the astral plane? That's the control plane on the Cisco back end with that intermittent system, etc. logs in. So anyways, I just wanted to use part of this article. Maybe you get a laugh at the Borg reference to the control plane, but also to illustrate that you have a lot of different people interconnected in these systems. That doesn't mean that they have front end, front haul access to your body. With that being said, declared and delineated with Cisco technology, we are now going to go into i.t. For government and public sector. Public sector i.t. At computerweekly.com. We're going to establish that computerweekly.com is an industry standard legacy net type of thing, network world, etc.. Oh, no, no, no. Talking about ransomware risks of i information technology management, leadership, efficacy legislation, regulation. If you're running a data center, you might have come across this usually in the format of a magazine in somebody's bathroom. Okay. Now this particular article is old enough, so we're going to talk about it just like it is. 2014 June 13th, 2014. Okay, here we go. Drone Kill Communications Net Illustrated Computer Weekly can illustrate how you can network connections or excuse me, Computer Weekly can illustrate how a UK network connection forms part of a US weapons targeting system that is slaughtered civilians and anti terrorist attacks gone wrong. The illustrations add credibility to a legal challenge begun last month over a 2012 contract. But we want to build the UK branch of the system of fiber optic network lying between Royal Air Force Crown in Northamptonshire, Surrey and Camp Lemonnier, a U.S. military base in Oh no. Did Djibouti Africa territory dominate? British officials have been slow to finger the Beattie contract under human rights rules because they said there was no evidence to suggest the UK connection was associated with drone strikes, let alone any that have gone wrong. There is, however, clear evidence that the UK connection excuse me with U.S. drone strikes, let alone any that had gone wrong. There is, however, clear evidence that the UK connection is part of a global intelligence and weapons targeting network that operate U.S. drone missions like a hand operates a puppet because that's how it works. The network was meant to make drone weapons targeting more accurate and to end catch fewer innocent people in the CROSSFIRE. But this network centric targeting also became the means of a chilling new type of warfare called targeted killing, computer driven intelligence led extrajudicial assassinations of suspected terrorists like those who kidnap schoolgirls in Nigeria and massacred shoppers in Kenya. The UK connection was part of this because under the targeted killing program, the network is the weapon designed to be utterly discriminative, but in practice not completely accurate. It had, according to the Bureau of Investigative Journalism, accidentally killed hundreds of civilians in 13 years of drone strikes on insurgents in fractured states in the Middle East, Asia and North Africa. The strikes have all but ceased in the mistakes reportedly led the U.S. to rein in the program. But the role of the U.K. connection remains the burning question. It will not only determine the outcome of a judicial review being sought in the U.K. by a Yemeni education official whose civilian, brother and cousin Ali and Saleem Al-khalili, cowardly, coldly were killed by a drone strike on their car in the Yemeni village of Sinan on the 23rd of January 2013. It will force the UK to base its part in the Killing program, and it will illuminate a frightening growth in the combined combined power of military and intelligence services to use the power of domineering surveillance to feed systems of automated targeting and killing. Network killing the mechanism of net centric warfare makes the idea that the U.K. connection is not facilitated. U.S. drone strikes absurd. The network made targeted killing possible. The network was also the basis of the mechanism that drove the actual strike operations. It carried the intelligence that selected the targets. It ran, the software that directed the operations. It incorporated the drones that carried out the strikes. The drones do not exist. A separate entity is called in to finish the job. The drones are nodes on the network. They are part of the network. The network is the weapon. The U.S. has been building its network to drive the systems in weapons, and particularly the drones that support its strategy of network centric warfare. The UK connection is part of this strategy. Drones rely on the network like trains rely on, tracks like puppets rely on strings. The networks give the drones their directions, distribute their surveillance, target their weapons. The blue map at the head of this article shows a map of the fiber optic core of this global network, the Defense Information Systems Network, as it stood in 2004. And this is what they show in It's very generic and kind of widest out for a reason rate security people sipper net. There you go. Okay. For this exam. Okay. Okay. The blue map at the head of this article shows a map of the fiber optic core of this global network, the Defense Information Systems Network, as it stood in 2004, showing the European branch of the network, The Blue Map depicts Royal Air Force Crown in Northamptonshire as a major junction of the Defense Information Systems network, then essential for carrying classified military

communications for the Secure Internet Protocol Router Network Simonet. It shows how Proton is connected to launch to Ramstein in Germany, the regional hub for the Stuttgart headquarters of U.S. Africa Command. It shows crowding also links to copied the Wait a minute additional. Yeah. Let's cut to the cappuccino. Look up at the channel depot. Did you know the communications hub in Naples, Italy, where the US Navy has its European and African command centers compared to Chino like Landstuhl? Ramstein connects to Bahrain, the base for us, CENTCOM in the Middle East. The blue map predates the UK connection to Djibouti, which VTR was contracted to provide in October 2012. Hey, I'm reading this by myself. Leave it alone. The contract specified a high bandwidth line between the UK and copied to Chino effectively an upgrade and then an extension to Djibouti, where Camp Lemonnier the Veneto was having bandwidth problems. When the Blue Map was published in 2004, the US military was working intensely to turn the dissent into the global surveillance and weapons targeting system it is today. Their efforts turned the Defense Intelligence System network into the backbone of a more extensive Department of Defense network called the global Information Grid Drone Net. Scientists and engineers from places such as the Massachusetts Institute of Technology, Lincoln Laboratory and MIT, Dutch Health and the National Security Agency. NSA modeled the gig on the Internet. It was a network of networks like the Internet. They joined the defense intelligence. If I say in that right, I don't know why that keeps tripping up in my brain. We're really seeing that, right? I think that is why I don't like the details. But, you know, I said, you stop. I'm sitting next to my coffee pot having to hold my head in place. And I looked at her to make sure I could show properly and.

Drone kill net part ii.MOV

Sabrina Wallace [00:00:00] Defense Information System Network. A lot of words. You're talking about things. It's all open source. And I'm allowed to look up definitions if you want. So we're going to make trouble. Call somebody as I'm busy. Okay. So there you go, The Defense Information System Network. All right. Okay. Back to my article. Having fun trying to pronounce all these words in order. Okay. So the Defense Information Systems Network turned into the global information grid. Drone net scientists and engineers from places such as MIT, El Al and the National Security Agency modeled the global information grid on the Internet. It was a network of networks like the Internet. They joined the Defense Information Systems Network, which still doing their own. I did it right. Oh, I'm going to listen harder for that because it's like a little jolt. And they join the defense information systems that work with satellite and radio to form a single seamless network. The U.S., DOD then strove to plug every device into it, every vehicle, every system, every drone to form one, all encompassing that. Yes. So now I was immune for you. Okay, we have no satcom concept. Come up for G.P.S., be M.S. Second, we allow us to be a Lewis relay tactical consumer unmanned ground systems and unmanned maritime systems. That means there's no men in there, manned aerial systems, somebody's kind of remote tactical consumer. That's your Stryker on the ground right there. Then we got the unmanned aerial to talk about those all the time in the tactical consumer psyche on the bottom with that gateway and distributed common ground system and baseline carriers and the people at the keyboards in the paired locations and your defense data centers and then know you're strategic consumers. Okay. High level. See for infrastructure. Hang on. I got there very high level. See for infrastructure, operational concept, graphic sensor data sensor data right there. The plan had both prosaic and transcendent aims at the work day level. US military and defense agencies didn't have enough bandwidth to support growing fleets of drones, let alone their emerging divisions of unmanned sea and land vehicles. Drones needed to descend to carry their control signals, as illustrated in the concept diagram above from the US Department of Defense Unmanned Systems Roadmap 2013 to 2038. It's fine. Now I'm busy. I'm still reading my fun article. The diagram illustrates how defense and intelligence agencies rely on the dissent as well, to gather data driven sensors such as video and infrared. The dissent carries drone data to systems such as the Distributed Common Ground System, the Common store of imagery intelligence for U.S. military and intelligence agencies, Satellite connection. The G.I.s and gig became more essential to drones as demands for their dense imagery, intelligence outgrew the satellite and terrestrial networks ability to deliver it. The U.S. undersecretary of defense used this diagram in 2008 that their means is safe to talk about. Yell. Okay. So what we were talking about earlier over here, it's your West Virginia mountain. Look. How is that them? They're electronic engineers. Yeah. We come here for our education. We're an Appalachian. Okay? Sometimes we need a picture to make it understandable that we've surrounded everybody with them. There's satellites, and then we shine a signal down to the ground. And then there's a man somewhere. He installing hardware or software to make

sure with the modular open system approach that these things here, that approach, they're going to shoot you in the nose. Error. 2.15.4802.15.5 Wireless sensor networks and then 802.15.6 broadcast across the body near field effect. We're going to electrocute your cells into submission for Bioelectric Biomedical A.I. Precision. It's all about your health care. Uh huh. That's why I'm reading over this in the way that I am with a little less sarcasm so that people can start to grasp the very serious nature of what I talk about on my channel and then decide how they would like to proceed accordingly. Okay. The U.S. undersecretary of Defense used this diagram in 2008 to illustrate how military and intelligence agencies use the gig global information grid to communicate via satellite with drones and deployed forces. High bandwidth satellite constellations are part of the plan. The quiet out there. It's all part of this. I'm reading the one show and transformational satellite was later supplanted by wideband global satcom. Well, how do you do Teleport? Oh. Oh, sorry. We're talking about the DSN and probably telepathy. The DSN was connected to satellite constellations through antenna called Teleports. Illustrated on the left by Johns Hopkins University Advanced Physics Laboratory. And that must be a secret name for Hogwarts, right? The US subsequently built teleports in eight locations. Oh, goodness. By Frame Wahiawa, Hawaii. Fort Buckner. Okinawa. Japan. Largo. Patricia, Italy. Landstuhl. Ramstein. Germany. Guam and the Philippines. Camp Roberts, California. And North West Virginia. Great Internet radio deployed forces were also connected to the gig with a radio system written and software communicating using the Internet protocol. And now we are to your Jtr. S networking at the Tactical Edge, which I've been here with some of the joint tactical radio systems, which is what put me in the P.W. or excuse me p0w stuff with the daisy researching and whatnot around the Army's information, the tactical radio, the joint Tactical radio system. JT RC was developed by an mit dash l l a uniquely, wholly military funded university department that in 2004 was responsible for developing major components for the gig and surveillance of weapons targeting technologies that would run over it. Predator The Predator strike drone relied on the gig descend to target its weapons as illustrated in the US Department of Defense Unmanned Aircraft Systems Roadmap 2005 to 2030. There were two ways of controlling a predator from a local station or one far away. Both relied on the gig descend when a remote pilot housed with deployed forces in the theater of operations forward operating location. Did the controlling the drone relied on the DSN to reach back to core military computer systems essential to its mission. The most essential computer system was the distributed common ground system. The descent in the DC gates were also essential, and the other primary predator predator control mode. In a remote split operation, the Predator would be launched from a line of sight control station near to its mission. Yes, I left some acronyms open for other folks, but Control would pass over to a remote pilot back in a fixed military base such as Nellis Air Force Base in Nevada. The drills control signals would have to be routed over the DSN to a Predator primary satellite link. So having said your phone itself, I got two homes in different area codes. You're wonder why I'm always singing. The drones control signals would have to be routed over the descend to a predator primary satellite link. So having pre dated development to the gig, the predator use proprietary network technology and outmoded asynchronous transfer mode ATM communications. This was handled by the D as an asynchronous transferred mode system d A-10s. But the old Predator comms system was a hindrance to the gig strategy. They were not Internet enabled. That meant they couldn't be assimilated into the gig. The aim of the gig was for every sensor, every weapon, every comms system, and every software program to operate using the Internet protocol. Any military resource would then be available for control or observation, for attack, or just for intelligence to anyone with access to a gig terminal anywhere in the world in real time. The difference between drones communicating over ATMs and drones communicating over the Internet enabled gig descent was like the difference between communicating via walkie talkie or running apps on your smartphone. Network interfaces. There's your but somewhere over here and that X marks the spot. Okay. A ten year plan. The D.O.D. had a ten year plan to get around the problem by gradually upgrading its drone comms infrastructure. The first step would connect drones to the gate by turning their satellite links into gate gateways. That was to be done by around about now. They would act like they were an integral part of the network. The drones would ultimately become internet enabled themselves. They would communicate as Internet nodes. Their onboard Internet routers would use any spare bandwidth to rule out other people's gate traffic. They would become part of the network. By the time the Department of Defense Unmanned Systems Integrated Roadmap 2013 2 to 2038 was published in December. U.S. drones were operating in the way illustrated in stage two in the diagram above. And drones were using network gateways to get their command instructions over the descent, it said. The descent likewise disseminated the surveillance data they picked up on their missions. Well, looky there, synergies. It's one of our favorite pictures

we've been using all along on my desktop. I like to read about satellites. It's interesting to me as a former network technician excuse me, network engineer, the power of the gig plan would follow in every drone, soldier, satellites, ship, drop gun and so on. So we're sharing their intelligence, the surveillance sensor data over it, the gig, the global information grid, as illustrated in the concept diagram above from the Department of Defense's 2007 K architectural vision. I'm so glad I used the right paperwork. They were all part of the gig. They all communicated using the same Internet protocol. They were all integral to the network building blocks. A common communications protocol laid the foundation for common data formats and common software interfaces. This was the transcendent aim of the gig. It allowed military assets to be available on the network as building blocks. The gig would be greater than the sum of its parts. This would theoretically make every chunk of intelligence data, every surveillance camera, every weapon, every software system as a building block on the gig net. Targeting that was the basis of net centric warfare, making everything available as a software service on the military Internet. Its most characteristic application was net centric targeting that involves combining different surveillance sensors and intelligence databases on the fly to get an automated fix on a target. The power of net centric targeting became apparent in simple tests. The combined just two airborne surveillance sensors. Each sensor had limited ability even to spot a target on its own, let alone get a fix. According to this graphic from a 2006 presentation by Colonel Tom Wozniak of U.S. Air Combat Command. Another side correlation function thing headed to the US Network Center Collaborative Targeting System Take sensor readings with a middling probability of making sense to a target computer and combines them to create a high probability fixes where they match. The NCS became operational in 2007 after years of development in collaboration with the UK, according to Diddy's statements to Congress. The preeminent application of net centric targeting is the one that made the US targeted killing program possible time critical or time sensitive? Time sensitive targeting. The graphic above shows how it usually takes hours for military personnel to plan a strike. They have to digest their battle plans for start, pour over maps and work out less, where then they have to find their target. That means of arranging for intelligence, reconnaissance and surveillance sensors to hunt for it. Sensor hunters, They have to collate all their intelligence and analyze the data. Then they have to calculate effects, nominate targets to be attacked, prioritize among them, coordinate their operations, find suitable weapons platforms, and get them to the target area. Account for weather, choose the best route to the target. Watch out for friendlies and when the strike has been made, assess the damage network targeting premise to do all of this in minutes by automating it semantic interoperability dynamically discover access Fuze fusion centers, multi source intelligence intelligence databases. Net centric targeting relies on a process called data fusion or semantic interoperability. That means storing your data in ways that can always be cross matched, not just military data. Net centric targeting. Developers wrote civil databases into their plans to such as immigration databases and feeds from civil intelligence agencies. Automated targeting combined with algorithms that watch for target signatures. This creates the means to spot targets on the fly vehicular ad hoc network on the fly, and it creates the means to spot targets as small and as fleeting as people and to kill them within minutes. As illustrated in the diagram above published in 2007, the year the U.S. network centric collaborative targeting system went into operational use by Computer Technology Associates, the defense and intelligence systems contractor that helped develop the system. The example describes the target signature. An algorithm tells the targeting system that in the event of an emergency, it should look out for a particular person known to the CIA as Target ID 1454 matrix C identifier. And I got two numbers, some more and showing synergies since last year. The targeting system keeps watch for them with its blue force and red force tracking systems. The military used these to track to trace the movements of those they've classified as goodies and baddies. The targeting system keeps track of immigration and airport databases as well. In the example, somebody on the red target list, the general hit list, has popped up in the immigration database. It checks to see if they match against CIA records. They do, and they match against the CIA file with the same target I.D. as specified in the target algorithm. Target ID 1454. The targeting system sends geographical coordinates to people in green uniforms, time sensitive, targeting this sort of computer vigilance combined with network intelligence, throw up new targeting possibilities. The U.S. started building common surveillance systems with its partners in the North Atlantic Treaty Organization, NAITO. The more sources of intelligence they had, more targets they could see. NAITO usually took days to plan a strike against even a fixed target. If it could do that, it's a good spot. Targets that were too elusive before these time sensitive targets could be threats that emerge so quickly that they had to be attacked within minutes if they were to be stopped or they could be lucrative targets that appeared to be in or excuse me, that appeared in the surveillance net only fleetingly and would

escape if they weren't attacked quickly. He gives friendly forces the option of striking targets minutes after they are in a fight, said this presentation by NATO's chief scientist in 2013. NATO's targeting the U.S. formed a coalition to develop a web of NATO's net centric targeting systems. It would get target intelligence on the fly from surveillance gathered by any number of NATO countries that happen to have forces, sensors or databases with something to add to the kill equation. The Multi Sensor Aerospace Crown, Joint Information Surveillance, Reconnaissance Interoperability Coalition Magic worked on making natal ISR sensors, produced data in the same formats. Magic aim to make innumerable surveillance platforms compatible Electro optical infrared synthetic aperture radar high resolution video are still images moving target indicators and electronic support measures. Their aim is what U.S. strategists call dominant battlespace awareness, having more eyes and ears, feeding more situational awareness back into the network than anybody else. Afghanistan Afghanistan strike. NATO's chief scientist gave a recent example of net centric targeting using its own test tool last year. The screenshot demonstrates a needle strike against armed opponents of its military invasion in Kabul, Afghanistan. It shows a map of Kabul with the location of the targeted people, as displayed in its test tool called Flexible Advanced Command and Control to. I went over this about a week ago. I think the difference between see to see 345 c 67 given ac6 and C five for sure. I didn't talk about seven very openly, I just made a joke about it. Advance C two services for NATO's joint time in sensitive targeting fast. This is the view that would appear on the computer screen of an intelligence officer, perhaps at a desk in digitally barring Stuttgart or Tampa, Florida. The intelligence officer has named his target terrorist group, meaning given a track identification code identifier z008 to distinguish it from other targets in the system. The software supports the Internet chat between military personnel overseeing the operation. This is the sort of communications handled by super net over the dissent. The fast tool handles multiple target tracks at the same time, and intelligence chief and other senior intelligence duty officer are also in the system pursuing tracks on Target zero four and zero five. Any word on the predators yet? Says a message from a chief of intelligence, surveillance, target acquisition and reconnaissance. An ICE star. E.T.A. Predators. 5 minutes, he is told. Just a minute before air traffic control sent a message saying an aircraft had been launched against another track, IDS 006. Kill chain computerizing weapons targeting involve breaking it up into a series of steps. It was systematic system. Systematized as business functions like purchasing and manufacturing were when they were computerized, where human actions were classified into distinct processes like produce, purchase orders, send invoice, receive goods. Time sensitive targeting is commonly known as the kill chain. This has six steps. Find, fix, track, target, engage and assess UK gizmo. The UK developed a system that needs and act with target data gleaned from conventional signals intelligence called Co-operative Electronic Support Measures Operation says assessment. Its target data is merged with other intelligence and CCTV. Anita Test assessment in 2005 produced this map allow showing line of bearing readings from ISR sensors, information surveillance, reconnaissance. Somebody out there got a notebook like pneumonia did in Georgia, write down a gazillion things and mile a minute each. Single B is a single signals intelligence reading from a surveillance aircraft. As expected, the test found a single reading was too unreliable to get a fix on an elusive target. Even a single aircraft with two LLB fixes would have to would have such a large error ellipse that it could not be used to target a weapon, said the narrow C three agency target leaked electronic emissions for less than 30 seconds and that NATO's test to zero five, the area of a poor target fixed called the error ellipse, was 11 kilometers by 600 meters, and that this was clearly far too large to risk an attack. But with five sensors on the lookout, they got to fix. Most of the data pertaining to SAS was classified, said a paper by the NATO's C three agency in 2007. But it said it is possible to show how SAS smoke and GEO locate targets that cannot be found by standalone operating Eland or ESM platforms. Target Intelligence. I'm going to do this really quick for people I can hear listening that are like that. Enterprise Service Management. Okay, good. Sam Right. Target intelligence. The U.S.? Well, yes. You electronic sensors, something or other. But I'm telling you, people are drowning me with acronyms because it's enterprise versus industrial to target intelligence. The U.S. military stores is our data and it's distributed common ground system. This is commonly described as the Imagery Intelligence store, queried by U.S. defense and intelligence agencies alike when planning operations, informing target tracks and fixes. Allied nations use it to as do targeting systems. It gives them a common view of the battlefield and everything on it. Common Ground. Common ground means the same surveillance from platforms such as drones, the same human intelligence, the same geolocation coordinates from target tracks, the same signals readings from sesame oil, the same aerial photography and satellite images, drone operations. This screenshot purports to be taken from a D.C. gas tool in 2003 when the system was still in early development.

The images of Croatia, Montenegro as IT Montenegro and Bosnia, Herzegovina and Herzegovina, Herzegovina and 30th of June, the day Croatian Defense Minister Convoy Antonov welcome the opening of NATO's expansion talks among former Yugoslavian states and Baltic countries. The spoke at the NATO's excuse me and spoke at the New Europe Euro-Atlantic Partnership Council. It shows the flight paths and surveillance nets of various aircraft, including Global Hawk and Predator drones. Time critical targeting was part of the disguise concept of operations, according to this 2007 presentation by net centric developer Computer Technology Associates. The image depicts Acer data stories being combined with civil and military intelligence databases known to create time sensitive target tracks and strikes UK drone intelligence. The UK has access to this device and data stored as well. Intelligence analysts at the Royal Air Force Base in Marlow, Norfolk use disguise imagery to direct UK operations in Afghanistan, said in Royal Air Force press release in 2011. The RDF was building real time interoperability with the dogs, it said. Analysts received feeds from the U.S. Distributed Common Ground, the system which provides globally networked intelligence, surveillance and reconnaissance capabilities. This is the first time that the UK will have the capability to provide Near-real-time imagery intelligence support to Afghanistan from the UK, it said. Murky area national intelligence agencies used the disguise as well, according to some descriptions of the system. That includes the CIA, which is reported to operate some of the controversial drone strikes. The last ten years have seen persistent references to the intelligence community as an influence and contributor to developments of the global information grid. Dcgi has net centric systems and intelligence sharing. The likelihood of the intelligence community's dependance on the DCI or the DSN cannot be ignored, Ghosh, the former chief scientist of DARPA, said in a 2005 speech that intelligence agencies were part of the DOD's cake vision. David Smith, the DCI consultant who worked on the DHS and Gig transformation, wrote in 2006 that it was driven by and would serve both the DOD and intelligence community. The U.S. established a unified Cross Domain Management Office in 2006 to address the needs of the DOD and the ICC to share information and bridge disparate networks, director Marianne Bailey said in a 2008 paper. DOD told Congress in 2006 the tests of the gate at the Naval Research Laboratory would in 2007 include end to end testing with Department of Defense, Intelligence, Community allied and coalition activities. The tests would incorporate Jtr s t set Teleport Geek Band with expansion and net centric enterprise services. Renee phase of the Neato Communications and Information Agency said in a 2007 paper that signals intelligence sharing systems would get developed now that the intelligence community had discovered their benefits. The US Undersecretary of Defense, Joint Defense Science Board Intelligence Science Board, said that in 2008 and investments for both the intelligence community and the DOD had created the network infrastructure. It said that excellent progress had already been made in aligning metadata data from various sources across the DOD and the intelligence community. D.O.D. Chief Information Officer John Grimes formally committed in 2008 to ensure information and network situational data sharing with the intelligence community. The DOD, Intel, IT and Intelligence Chief Information officers also formally agreed to recognize one another's network security accreditations. DOD told Congress in 2009 that it was cooperating with intelligence agencies on the development of its net centric systems. Minor Corp., a company that did software engineering on the DCG, has helped develop NAITO ISR data standards and worked with Magic said in a 2009 paper about net centric enterprise systems that U.S. intelligence agencies used them to. 0dd harmonized its i.t standards and architectural processes with federal and intelligence agencies and coalition allies. In 2010, it told Congress in 2011, the alignment was done under the Command Information Superiority Architecture program. The Secretary of Defense Office formed to develop the architecture and that centric reference model. The U.S. Navy told Congress in 2011 it was developing a system to fuze biometric data it took from people and ships. It board with intelligence community counterterrorism databases. DISA implemented an intelligence community system in 2011 that exposed DOD data to users with appropriate security clearance, it said in its Convergence Master Plan 2012, it told Congress in 2012 the design carried information for the DOD intelligence community and other federal agencies. United States Air Force Major General Craig eight Frank Franklin, vice director of Joint Staff, issued an order in 2012 specifying conditions for the intelligence community to connect to the gate and for ICI systems to connect to the collateral DSN systems. He charged the U.S. DMO with establishing cross domain computer services between the DOD and intelligence community. The U.S. DMO simultaneously published a list of network services that would work across DOD and intelligence domains. The National Geospatial Intelligence Agency said in 2012 it had aggressively broken barriers to imagery intelligence data sharing between civil defense and intelligence agencies. The US Navy said in its 2013 program Guide the next increment of its portion of the D.C. GSD stash and would leverage both DOD and

intelligence community hardware and software infrastructures. It said upgrades on the areas to aircraft, its premier manned ISR and targeting platform would enable continued alignment with the intelligence community. Theresa Takai, D.O.D. Chief Information Officer, ordered in 2013 that all DOD systems would be made interoperable with the intelligence community. She committed formerly to agree metadata standards with the intelligence community, to share them, to agreement on data standards with the intelligence community, ICAO, And she formally requested agencies in the government departments, including the CIA, Treasury Department of Justice, Nersa and the Department of Transport, agree cybersecurity procedures for connecting to the cyber net by June 2014, the NGV said in its 2013 update to the National Imagery Transmission Format Standard. And it or excuse me, slash as the developments had been driven in recent years by a need to share intelligence data between the DOD and intelligence community. It was developed in collaboration with DOD Intelligence Community, NATO's Allied Nations Technical Bodies and the Private Sector Intelligence Community is an official designation of 17 agencies for the U.S. Director of National Intelligence. That includes the CIA, FBI, Department of Homeland Security, Treasury, Drug Enforcement Administration, Departments of Energy and State, Coast Guard, NSA, and intelligence agencies associated with each of the U.S. military forces. The progress Internet centric integration appears from public records to have been long, arduous, partial, reluctant, ongoing, yet undeniable. Even if the CIA has been averse to conducting its drone operations directly over the years, and it is unlikely the DOD network has not carried intelligence and other data essential to its missions in Yemen and everywhere. The CIA was directly associated with a more recent evolution of the D.C. Central Intelligence Agency.

Drone kill net part iii.MOV

Sabrina Wallace [00:00:01] A more substantial computer framework for sharing data between defense and intelligence agencies and their international allies, called the Defense Intelligence Information Enterprise has subsumed the disguise at the heart of D.I. To ease the disguise integration backbone, a set of data fusion services said in a 2012 overview Overview by the DCG. S Multi Execution Team office at Hanscom Air Force Base, Massachusetts, to have delivered a system for the DOD and intelligence community to search, discover and retrieve its disguise content. United States Air Force characterized it as a cross domain service. The ITU ea delivered a plethora of cross domain services for net centric missions as part of the DOD, as part of the Department of Defense Architecture framework in 2020 ten. Listed in the flesh pink graphic above, which links to a sheet given to developers who attended a May 2013 DOD slash icy slugfest and mash up at George Mason University. Virginia Censor and target planning are included in the list of mission services on the sheet. A collection over 150 net centric software services called the Die to ease service the dash for services functionality description. They also include SIGINT, pattern matching, target validation, entity activity patterns and identity disambiguation for human intelligence, HUMINT, and intelligence preparation of the battlefield. This is a defense intelligence initiative. That means it comes under the direct remit of the defense intelligence agencies. But as always, it is described as for the benefit of both the DOD and the wider intelligence community. The undersecretary of the Defense for Intelligence published a diagram of the stakeholders stakeholders in D2 ea in a presentation last year. D2 II was owned by Defense Intelligence for the CIA and other intelligence agencies used in the U.S. military was, meanwhile reported to have stopped sending drones over Yemen in April. The CIA was said to have continued, but from an erstwhile secret base in Saudi Arabia, even when drone attacks on Yemen were reportedly launched from Djibouti, the picture was murky enough for UK officials to dismiss a complaint by legal charity Reprieve that the UK connection made B.T. and its contractor answerable for resulting civilian deaths. The conflation of military commands around Yemen was complicated. It was hard to point at a drone strike and say who launched it from where? With comms directed down what the U.S. wouldn't say VTI. It ignored the question. U.S. CENTCOM, the military group that invaded Iraq, ran lemonnier until October 2008 when it handed control to U.S. AFRICOM. CENTCOM kept Yemen as an operational area, but its base in Bahrain was almost 1000 miles away. AFRICOM kept Yemen as an area of interest. Lemonnier was separated from Yemen by a finger of water just 20 miles across called the Bab el Mandeb Strait. Reports continue to cite Lemonnier as a launch site of lethal targeting drone missions. U.S. AFRICOM would not tell Computer weekly what drove missions launched from Lebanon, not even when whether they did nor what mission support it gave CENTCOM, nor whether it did, nor whether CENTCOM. It continued operating from Lemonnier after command as to AFRICOM, nor whether

AFRICOM carried out missions in Yemen under CENTCOM's command, U.S. AFRICOM spokesman Army Major Fred Harrell said of a lot of assumptions were made about what the drone strikes. But like the White House, he refused to clarify who, what, where, when. But he did confirm that CENTCOM coordinated Yemen operations with Djibouti. Our area of responsibility, Porter said of CENTCOM and also U.S. European Command, said Harel. So it seemed to say that anything that occurs across what we call the seam between where our area of responsibility ends or where there starts, there's always a coordination between combatant commanders on what goes on. We do coordinate with our neighbor combatant command, such as European Command and CENTCOM. This article is illustrated in fully how such coordination is conducted over the DSN. Earlier reports in Computer Weekly described how a 2012 DSN upgrade 11 year coincided with the Beatty contract to extend the line from provided in a 2012 DSN upgrade in Stuttgart and how an intelligence contractor was hiring analysts to work on targeting systems over the descent from Stuttgart drone video feeds. Upgrades including the UK connection and made the U.S. network wide enough to yet another development in drone targeting and intelligence. Real time video feeds Jesus Unified Video Dissemination service takes live video streams from Predator and Reaper drones and transmits them via teleports such as those descend com hubs in Naples and Landstuhl in Bahrain. UAV video gets streamed via the teleports and over the descend, according to the graphic below from the DOD 2013 to the 2028 Unmanned Systems Road Map. The graphic illustrates how their imagery is stored in the DCS and in the archives at the NSA from a DC presentation last year. It illustrates how the whole system depends on the DSN. It shows drones and surveillance aircraft associated with Camp Lemonnier, otherwise known as the headquarters of Combined Joint Task Force Horn of Africa under U.S. AFRICOM. The drones feed their video streams via a wide band satellite back to Lemonnier as well as a nearby decent trunk gateway. A teleport. D.O.T. records occasionally state that its net centric and descend investments aim to give simultaneous views of the battlespace to any personnel or commanders anywhere in the world. This was, for example, one reason given for the disinvestment eliminate. The idea was that it might help commanders at bases in different places like Bahrain and Djibouti, and commands with different headquarters in places like Stuttgart and Tampa and perhaps even intelligence analysts in different domains to coordinate their missions. Streaming drone video was a part of that. Drone over IP, the DSN corps built with trunk lines like the ones between Djibouti and the U.K., provided the basis of drone over Internet protocol. As of all the other net centric services, it would allow staff in different locations to use the same systems to see the same intelligence collaborate in the same operations. Operational ARPANET Architecture Design Core Fiber network looks like the lost their image there is hence at the center of this network diagram showing how the unified video dissemination service operated in 2012. The diagram shows video feeds running from drones over satellite links and finally via teleports over the DSN. The teleports at logger Patricia Italy in Landstuhl, Germany, are shown distributing live video feeds to the and the Italian teleport on the descent between the UK and Djibouti were made capable of live drone video comes in May 2012, the year BT was contracted to make the UK connection. The diagram Notes, published in December 2013 of the DOD's 2013 2038 Unmanned Systems Roadmap. It shows how a full motion drone video is carried across the network to used as storage points where they can be made available to users on cyber net. The graphic shows two distinct components the part in green that gets the full motion video to the network and the part in red that makes the video available to military users and their systems. Both parts operate over the descent DC and in this diagram, Link Satcom is directed through teleports with theater communications for bases such as the one in Djibouti. It links those with the classified cyber network that also runs over the descent. And with UAV systems operating from decent regional computing centers called Defense Enterprise Computing Centers, Network Infrastructure. The network components in the diagram above match both those described in the official notice that described its contract for the UK connection in 2012 and the U.S. Navy's congressional budget justifications that describe the same device and connection upgrade as an operational need for delivery. The key components are the MSP Multi-Service provisioning platform, a device to connect the device on line at bases such as Camp Lemonnier and another familiar term to the synergies. Hape High assurance Internet protocol encryptor encryption devices. These were devices specified in U.S. Congressional justifications for building the descent into the gig MSP devices for the major junctions of the global information grid, as illustrated in this graphic from a 2004 presentation by Frank Crist, then director of communications programs for the U.S. Office of the Secretary of Defense. The diagram shows the gig test environment most likely operated by NRL in 2004. It portrays components that would later be used to build the gig in the real world. The network infrastructure specified for Beattie's UK connection was also illustrated in this

diagram from an article in the summer 2006 DOD Information Assurance Newsletter. It illustrates the gig bandWith Expansion program, a scheme to upgrade the gig for net centric warfare and to carry the imagery intelligence spewed out by burgeoning numbers of drones. The new device and infrastructure would include O.S. 192 Fiber Optic Cables, Odyssey and MSP network devices, and CG class, high speed, high assurance Internet protocol, HAPE devices, all devices specified by contract for the UK to Djibouti connection in all matching U.S. budget jurisdictions. Excuse me justifications for expenditure with the expanded bandwidth provided by gig Ashby DC can address high capacity applications e.g. imaging, video streaming and provide a higher degree of network security and integrity, said David Smith, DHS and program manager wrote the article. The program is the first of its kind to bring high speed, high assurance Internet protocol encrypted devices to a dirty network. The hip devices introduced because of the NSA's anticipatory development will greatly increase the ability to bring secure, net centric capabilities to the intelligence community in DOD operations. David said that he has consistently said it could not be held responsible for what anybody did with the communications infrastructure it supplied, but can categorically state that the communication system mentioned in the previous complaint is a general purpose fiber. Object system. It has not been specifically designed or adapted by BT for military purposes. BT has no knowledge of the reported U.S. drone strikes and no involvement in any such activities. Just if I were you. That's me on the end, said a spokesman for BT in response to questions earlier this year and after reading for almost 40 straight minutes. I hope those of you out there understand there's not a word of this article I don't know about, haven't already showed to people. And now I'm going to briefly, since we're a 10 minutes drop down here to prove that electronic warfare JPEGs and I'm going to pull which one first. Here are those of the other ones. Hang on, hang on. Oh, come on. Where's my cool little picture and my satellites and stuff? That's not the one. And then the notes and the cell. No, that's all of their video game controllers. Danny's out there somewhere laughing, and I got to get back to the machine, learning for other things. And there's smart cities and the grids in the Nano. And I told people I'd come back and talk about all this crap with channel bonding as it's part of how they're doing the HPC and going through this four layers because they're not subtle and they're using them for all sorts of crap sake now. Yeah, I don't know. Where did I put that one? I'm not sure. Okay, well, then I'm going to go back real quick here. And now I'm going to close up making a quick video short.