By William M. Arkin

From Newsweek | Original Article

To watch video and see the photos, click here.

The largest undercover force the world has ever known is the one created by the Pentagon over the past decade. Some 60,000 people now belong to this secret army, many working under masked identities and in low profile, all part of a broad program called "signature reduction." The force, more than ten times the size of the clandestine elements of the CIA, carries out domestic and foreign assignments, both in military uniforms and under civilian cover, in real life and online, sometimes hiding in private businesses and consultancies, some of them household name companies.

The unprecedented shift has placed an ever greater number of soldiers, civilians, and contractors working under false identities, partly as a natural result in the growth of secret special forces but also as an intentional response to the challenges of traveling and operating in an increasingly transparent world. The explosion of Pentagon cyber warfare, moreover, has led to thousands of spies who carry out their day-to-day work in various made-up personas, the very type of nefarious operations the United States decries when Russian and Chinese spies do the same.

Newsweek's exclusive report on this secret world is the result of a two-year investigation involving the examination of over 600 resumes and 1,000 job postings, dozens of Freedom of Information Act requests, and scores of interviews with participants and defense decision-makers. What emerges is a window into not just a little-known sector of the American military, but also a completely unregulated practice. No one knows the program's total size, and the explosion of signature reduction has never been examined for its impact on military policies and culture. Congress has never held a hearing on the subject. And yet the military developing this gigantic clandestine force challenges U.S. laws, the Geneva Conventions, the code of military conduct and basic accountability.

The signature reduction effort engages some 130 private companies to administer the new clandestine world. Dozens of little known and secret government organizations support the program, doling out classified contracts and overseeing publicly unacknowledged operations. Altogether the companies pull in over $900 million annually to service the clandestine force—doing everything from creating false documentation and paying the bills (and taxes) of individuals operating under assumed names, to manufacturing disguises and other devices to thwart detection and identification, to building invisible devices to photograph and listen in on activity in the most remote corners of the Middle East and Africa.

Special operations forces constitute over half the entire signature reduction force, the shadow warriors who pursue terrorists in war zones from Pakistan to West Africa but also increasingly work in unacknowledged hot spots, including behind enemy lines in places like North Korea and Iran. Military intelligence specialists—collectors, counter-intelligence agents, even linguists—make up the second largest element: thousands deployed at any one time with some degree of "cover" to protect their true identities.

The newest and fastest growing group is the clandestine army that never leaves their keyboards. These are the cutting-edge cyber fighters and intelligence collectors who assume false personas online, employing "nonattribution" and "misattribution" techniques to hide the who and the where of their online presence while they search for high-value targets and collect what is called "publicly accessible information"—or even engage in campaigns to influence and manipulate social media. Hundreds work in and for the NSA , but over the past five years, every military intelligence and special operations unit has developed some kind of "web" operations cell that both collects intelligence and tends to the operational security of its very activities.

In the electronic era, a major task of signature reduction is keeping all of the organizations and people, even the automobiles and aircraft involved in the clandestine operations, masked. This protective effort entails everything from scrubbing the Internet of telltale signs of true identities to planting false information to protect missions and people. As standard unforgettable identification and biometrics have become worldwide norms, the signature reduction industry also works to figure out ways of spoofing and defeating everything from fingerprinting and facial recognition at border crossings, to ensuring that undercover operatives can enter and operate in the United States, manipulating official records to ensure that false identities match up.

Just as biometrics and "Real ID" are the enemies of clandestine work, so too is the "digital exhaust" of online life. One major concern of counter-terrorism work in the ISIS age is that military families are also vulnerable—another reason, participants say, to operate under false

identities. The abundance of online information about individuals (together with some spectacular foreign hacks) has enabled foreign intelligence services to better unmask fake identities of American spies. Signature reduction is thus at the center of not only counter-terrorism but is part of the Pentagon's shift towards great power competition with Russia and China—competition, influence, and disruption "below the level of armed conflict," or what the military calls warfare in the "Gray Zone," a space "in the peace-conflict continuum."

One recently retired senior officer responsible for overseeing signature reduction and super-secret "special access programs" that shield them from scrutiny and compromise says that no one is fully aware of the extent of the program, nor has much consideration been given to the implications for the military institution. "Everything from the status of the Geneva Conventions—were a soldier operating under false identity to be captured by an enemy—to Congressional oversight is problematic," he says. He worries that the desire to become more invisible to the enemy not just obscures what the United States is doing around the world but also makes it more difficult to bring conflicts to a close. "Most people haven't even heard of the term signature reduction let alone what it creates," he says. The officer spoke on condition of anonymity because he is discussing highly classified matters.

The secret life of Jonathan Darby

Every morning at 10:00 a.m., Jonathan Darby embarks on his weekly rounds of mail call. Darby is not his real name, but it is also not the fake name on his Missouri driver's license that he uses to conduct his work. And the government car he drives, one of a fleet of over 200,000 federal vehicles owned by the General Services Administration, is also not registered in his real or his fake name, and nor are his magnetically attached Maryland state license plates really for his car, nor are they traceable back to him or his organization. Where Darby works and the locations he visits are also classified.

Darby's retired from the Army, and he asks that neither his real nor his cover name be used. He served for 20 years in counterintelligence, including two African assignments where he operated in low profile in Ethiopia and Sudan, masquerading as an expat businessman. Now he works for a Maryland-based signature reduction contractor that he asked *Newsweek* not to identify.

As Darby makes his rounds to some 40 or so post offices and storefront mailbox stores in the DC Metropolitan area, he picks up a trunk full of letters and packages, mailing a similar number

from rural addresses. Back at the office, he sorts through the take, delivering bills to the finance people and processing dozens of personal and business letters mailed from scores of overseas locations. But his main task is logging and forwarding the signature reduction "mechanisms" as they are called, passports and State driver's licenses for people who don't exist, and other papers—bills, tax documents, organization membership cards—that form the foundation of fake identities.

To register and double-check the authenticity of his daily take, Darby logs into two databases, one the Travel and Identity Document database, the intelligence community's repository of examples of 300,000 genuine, counterfeit and altered foreign passports and visas; and the other the Cover Acquisition Management System, a super-secret register of false identities where the "mechanisms" used by clandestine operators are logged. For false identities traveling overseas, Darby and his colleagues also have to alter databases of U.S. immigration and customs to ensure that those performing illicit activities can return to the United States unmolested.

For identity verification, Darby's unit works with secret offices at Homeland Security and the State Department as well as almost all 50 states in enrolling authentic "mechanisms" under false names. A rare picture into this world came in April 2013 when an enterprising reporter at Northwest Public Broadcasting did a story suggesting the scale of this secret program. His report revealed that the state of Washington alone had provided hundreds of valid state driver licenses in fictitious names to the federal government. The existence of the "confidential driver license program," as it was called, was unknown even to the governor.

Before the Internet, Darby says—before a local cop or a border guard was connected to central databases in real time—all an operative needed to be "undercover" was an ID with a genuine photo. These days, however, especially for those operating under deep cover, the so-called "legend" behind an identity has to match more than just a made-up name. Darby calls it "due diligence": the creation of this trail of fake existence. Fake birthplaces and home addresses have to be carefully researched, fake email lives and social media accounts have to be created. And those existences need to have corresponding "friends." Almost every individual unit that operates clandestinely—special operations, intelligence collections, or cyber—has a signature reduction section, mostly operated by small contractors, conducting due diligence. There they adhere to what Darby calls the six principles of signature reduction: credibility, compatibility, realism, supportability, verity and compliance.

Compliance is a big one, Darby says, especially because of the world that 9/11 created, where checkpoints are common and nefarious activity is more closely scrutinized. To keep someone

covert for real, and to do so for any period of time, requires a time consuming dance that not only has to tend to someone's operational identity but also maintain their real life back home. As Darby explains it, this includes clandestine bill paying but also working with banks and credit card security departments to look the other way as they search for identity fraud or money laundering. And then, signature reduction technicians need to ensure that real credit scores are maintained—and even real taxes and Social Security payments are kept up to date—so that people can go back to their dormant lives when their signature reduction assignments cease.

Darby's unit, originally called the Operational Planning and Travel Intelligence Center, is responsible for overseeing much of this (and to do so it operates the Pentagon's largest military finance office), but documentation—as important as it is—is only one piece of the puzzle. Other organizations are responsible for designing and manufacturing the custom disguises and "biometric defeat" elements to facilitate travel. Darby says this is where all the Special Access Programs are. SAPs, the most secret category of government information, protect the methods used—and the clandestine capabilities that exist—to manipulate foreign systems to get around seemingly foolproof safeguards including fingerprinting and facial recognition.

'Signature reduction' is a term of art

Numerous signature reduction SAPs, programs with names like Hurricane Fan, Island Hopper and Peanut Chocolate, are administered by a shadowy world of secret organizations that service the clandestine army—the Defense Programs Support Activity, Joint Field Support Center, Army Field Support Center, Personnel Resources Development Office, Office of Military Support, Project Cardinals, and the Special Program Office.

Befitting how secret this world is, there is no unclassified definition of signature reduction. The Defense Intelligence Agency—which operates the Defense Clandestine Service and the Defense Cover Office—says that signature reduction is a term of art, one that "individuals might use to ... describe operational security (OPSEC) measures for a variety of activities and operations." In response to *Newsweek* queries that point out that dozens of people have used the term to refer to this world, DIA suggests that perhaps the Pentagon can help. But the responsible person there, identified as a DOD spokesperson, says only that "as it relates to HUMINT operations"—meaning human intelligence— signature reduction "is not an official term" and that it is used to describe "measures taken to protect operations."

Another senior former intelligence official, someone who ran an entire agency and asks not to be named because he is not authorized to speak about clandestine operations, says that signature reduction exists in a "twilight" between covert and undercover. The former, defined in law, is subject to presidential approval and officially belongs to the CIA's National Clandestine Service. The latter connotes strictly law enforcement efforts undertaken by people with a badge. And then there is the Witness Protection Program, administered by the U.S. Marshals Service of the Justice Department, which tends to the fake identities and lives of people who have been resettled in exchange for their cooperation with prosecutors and intelligence agencies.

The military doesn't conduct covert operations, the senior former official says, and military personnel don't fight undercover. That is, except when they do, either because individuals are assigned—"sheep dipped"—to the CIA, or because certain military organizations, particularly those of the Joint Special Operations Command, operate like the CIA, often alongside them in covert status, where people who depend on each other for their lives don't know each other's real names. Then there are an increasing number of government investigators—military, FBI , homeland security and even state officials—who are not undercover per se but who avail themselves of signature reduction status like fake IDs and fake license plates when they work domestically, particularly when they are engaged in extreme vetting of American citizens of Arab, South Asian, and increasingly African background, who have applied for security clearances.

'Get Smart'?

In May 2013, in an almost comical incident more reminiscent of "Get Smart" than skilled spying, Moscow ordered a U.S. embassy "third secretary" by the name of Ryan Fogle to leave the country, releasing photos of Fogle wearing an ill-fitting blond wig and carrying an odd collection of seemingly amateurish paraphernalia—four pairs of sunglasses, a street map, a compass, a flashlight, a Swiss Army knife and a cell phone—so old, one article said, it looked like it had "been on this earth for at least a decade."

The international news media had a field day, many retired CIA people decrying the decline of tradecraft, most of the commentary opining how we'd moved on from the old world of wigs and fake rocks, a reference to Great Britain admitting just a year earlier that indeed it was the owner of a fake rock and its hidden communications device, another discovery of Russian intelligence in Moscow.

Six years later, another espionage case hit the news, this time when a jury sent former American military intelligence officer Kevin Patrick Mallory to 20 years in prison for conspiring to sell secrets to China. There was nothing particularly unique about the Mallory case, the prosecution making its own show of presenting the jury with a collection of wigs and fake mustaches looking like Halloween costumes, the whole thing seemingly another funny episode of clumsy disguise.

And yet, says Brenda Connolly (not her real name), one would be naïve to laugh too hard, for both cases provide a peek into the new tricks of the trade and the extreme secrecy that hides them. Connolly started her engineering career at the Directorate of Science and Technology at the CIA and now works for a small defense contractor that produces the gizmos—think "Q" in the James Bond movies, she says—for signature reduction operations.

That "ancient" Nokia phone carried by Ryan Fogle, she says, was nothing of the sort, the innocuous outsides concealing what she calls a "covert communications" device inside. Similarly, entered in evidence in Mallory case was a Samsung phone given to him by Chinese intelligence that was so sophisticated that even when the FBI cloned it electronically, they could not find a hidden partition used to store secrets and one that Mallory ultimately had to reveal to them.

Lost in the spy-vs-spy theater of both cases were other clues of modern signature reduction, Connolly says. Fogle also carried an RFID shield, a radio frequency identification blocking pouch intended to prevent electronic tracking. And Mallory had vials of fake blood provided by China; Connolly would not reveal what it would be used for.

Like many people in this world, Connolly is a connoisseur and curator. She can talk for hours about the broadcasts that used to go out from the Soviet Union—but also were transmitted from Warrenton, Virginia—female voices reciting random numbers and passages from books that agents around the world would pick up on their shortwave radios and match to prearranged codes.

But then Internet cafes and online backdoors became the clandestine channels of choice for covert communications, largely replacing shortwave—until the surveillance technologies (especially in autocratic countries) caught up and intelligence agencies acquired an ability not only to detect and intercept internet activity but also to intercept every keystroke of activity on a remote keyboard. That ushered in today's world of covert communications or COVCOMM, as

insiders call it. These are very special encryption devices seen in the Fogle and Mallory cases, but also dozens of different "burst mode" transmitters and receivers secreted in everyday objects like fake rocks. All an agent or operator needs to activate communications with these COVCOMMs in some cases is to simply walk by a target receiver (a building or fake rock) and the clandestine messages are encrypted and transmitted back to special watch centers.

"And who do you think implants those devices?" Connolly asks rhetorically. "Military guys, special ops guys working to support even more secretive operations." Connolly talks about heated fabrics that make soldiers invisible to thermal detection, electric motorcycles that can silently operate in the roughest terrain, even how tens of feet of wires are sown into "native" clothing, the South Asian shalwar kameez, the soldiers themselves then becoming walking receivers, able to intercept nearby low-power radios and even cell phone signals.

Fake hands, fake faces

Wigs. Covert communications devices. Fake rocks. In our world of electronic everything, where everything becomes a matter of record, where you can't enter a parking garage without the license plate being recorded, where you can't check in for a flight or a hotel without a government issued ID, where you can't use a credit card without the location being captured, how can biometrics can be defeated? How can someone get past fingerprint readers?

In 99 out of 100 cases, the answer is: there is no need to. Most signature reduction soldiers travel under real names, exchanging operational identities only once on the ground where they operate. Or they infiltrate across borders in places like Pakistan and Yemen, conducting the most dangerous missions. These signature reduction missions are the most highly sensitive and involve "close in" intelligence collection or the use of miniaturized enemy tracking devices, each existing in their own special access programs—missions that are so sensitive they have to be personally approved by the Secretary of Defense.

For the one percent, though, for those who have to make it through passport control under false identities, there are various biometrics defeat systems, some physical and some electronic. One such program was alluded to in a little noticed document dump published by Wikileaks
in early 2017 and called "Vault 7": over 8,000 classified CIA tools used in the covert world of electronic spying and hacking. It is called ExpressLane, where U.S. intelligence has embedded malware into foreign biometrics and watchlist systems, allowing American cyber spies to steal

foreign data.

An IT wizard working for Wikileaks in Berlin says the code with ExpressLane suggests that the United States can manipulate these databases. "Imagine for a moment that someone is going through passport control," he says, hesitant to use his real name because of fear of indictment in the United States. "NSA or the CIA is tasked to corrupt—change—the data on the day the covert asset goes through. And then switch it back. It's not impossible."

Another source pointed to a small rural North Carolina company in the signature reduction industry, mostly in the clandestine collection and communications field. In the workshop and training facility where they teach operators how to fabricate secret listening devices into everyday objects, they are at the cutting edge, or so their promotional materials say, a repository for molding and casting, special painting, and sophisticated aging techniques.

This quiet company can transform any object, including a person, as they do in Hollywood, a "silicon face appliance" sculpted to perfectly alter someone's looks. They can age, change gender, and "increase body mass," as one classified contract says. And they can change fingerprints using a silicon sleeve that so snugly fits over a real hand it can't be detected, embedding altered fingerprints and even impregnated with the oils found in real skin. Asked whether the appliance is effective, one source, who has gone through the training, laughs. "If I tell you, I'll have to kill you."

In real life, identity theft (mostly by criminals' intent on profit) remains an epidemic that affects everyone, but for those in the intelligence and counter-terrorism worlds, the enemy is also actively engaged in efforts to compromise personal information. In 2015, the Islamic State posted the names, photos and addresses of over 1,300 U.S. military personnel, instructing supporters to target and kill the identified individuals. The FBI said that the release was followed by suspected Russian hackers who masqueraded as members of ISIS and threatened military families through
Facebook
. "We know everything about you, your husband and your children," one menacing message said.

Counterintelligence and OPSEC officials began a large-scale effort to inform those affected but also to warn military personnel and their families to better protect their personal information on social media. The next year, ISIS released 8,318 target names: the largest-ever release until it

was topped by 8,785 names in 2017.

It was revealed that military personnel sharing location information in their fitness devices were apparently revealing the locations of sensitive operations merely by jogging and sharing their data. "The rapid development of new and innovative information technologies enhances the quality of our lives but also poses potential challenges to operational security and force protection," U.S. Central Command said in a statement at the time to the *Washington Post.*

Then came the DNA scare, when Adm. John Richardson, then chief of naval operations, warned military personnel and their families to stop using at-home ancestry DNA test kits. "Be careful who you send your DNA to," Richardson said, warning that scientific advancements would be able to exploit the information, creating more and more targeted biological weapons in the future. And indeed in 2019, the Pentagon officially advised military personnel to steer clear of popular DNA services. "Exposing sensitive genetic information to outside parties poses personal and operational risks to Service members," said the memo, first reported by Yahoo news.

"We're still in the infancy of our transparent world," says the retired senior officer, cautioning against imagining that there is some "identity gap" similar to the "bomber gap" of the Cold War. "We're winning this war, including on the cyber side, even if secrecy about what we are doing makes the media portrayal of the Russians again look like they are ten feet tall."

He admits that processing big data in the future will likely further impinge on everyone's clandestine operations, but he says the benefits to society, even narrowly in just making terrorist activity and travel that much more difficult, outweigh the difficulties created for military operational security. The officer calls the secrecy legitimate but says that the Defense Department leadership has dropped the ball in recognizing the big picture. The military services should be asking more questions about the ethics, propriety and even legality of soldiers being turned into spies and assassins, and what this means for the future.

Still, the world of signature reduction keeps growing: evidence, says the retired officer, that modern life is not as transparent as most of us think.