**When the homefront becomes the (cyber) front line**

By Col. Sarah Albrycht 4 Feb 2020

<https://www.fifthdomain.com/opinion/2020/02/03/when-the-homefront-becomes-the-cyber-front-line/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2002.04.20&utm_term=Editorial%20-%20Early%20Bird%20Brief>



*A Sailor assigned to the Los Angeles-class attack submarine USS Newport News (SSN 750) receives kiss from a loved one, at Naval Station Norfolk, after returning from a seven month deployment to the U.S. 6th Fleet area of operations. Newport News was the third ship of the United States Navy to be named for Newport News, Virginia. The contract to build her was awarded to Newport News Shipbuilding and Dry Dock Company in Newport News, on 19 April 1982, her keel was laid down on 3 March 1984, and commissioned on 3 June 1989. (Chief Mass Communication Specialist Darryl Wood/Navy)*

American soldiers have long marched off to war with one assurance: by fighting abroad they were keeping their families safe at home. Today, advances in digital technology combined with unregulated data collection threaten to make the homefront the military’s new front line. The ability to target military families using their digital footprint significantly alters the risk of military service and potentially changes the calculus of war.

Recently, Military Times [reported](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.wral.com%2Ffort-bragg-families-of-deployed-soldiers-troubled-by-menacing-messages-on-social-media%2F18892437%2F&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710466662&sdata=OJvOT5BA9LBLl1%2FSM49bO7czBufca3w2XcRbL6OHNf0%3D&reserved=0) that military family members of soldiers deployed in Kuwait had received “menacing messages” via social media that appeared to target families of the 82nd Airborne Division. An unnamed source believed that the family members had been identified through a hacked internet service provider at the forward location.

This is not the first time service members or their families have been [targeted](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Ffederalnewsnetwork.com%2Fgovernment-news%2F2018%2F05%2Frussians-posed-as-is-hackers-threatened-us-military-wives%2F&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710476658&sdata=V%2BC%2BRXZZL60vpH%2FNN4PiOngXPFg9ugItVqpADb2E0%2Fg%3D&reserved=0) in this [fashion](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fidentity.utexas.edu%2Fid-perspectives%2Fisis-targeting-military-members-via-social-media&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710486656&sdata=RloXVXn1TlBHkRI53wKaxKY%2BGD9DS02N%2BH7RRANwwjE%3D&reserved=0) and reflects a trend of threats that are not receiving enough attention. The larger a person’s digital footprint, the more vulnerable they and their families are to being targeted.

What happens when our digital footprint moves from being used to develop targeted advertisements and digital services, to being used to target individuals as an act of terror or war? While this incident looks like a fairly simple hack of email data, when considered in the light of other [news](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.washingtonpost.com%2Fnation%2F2019%2F12%2F12%2Fshe-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter%2F%3Farc404%3Dtrue&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710486656&sdata=HJCQCATBRrSQymiKhYG5Iz8RhMH20llAE%2B%2BKkSGHE2g%3D&reserved=0) stories that demonstrate the ability to target individuals by exploiting a digital vulnerability, it takes on a [frightening](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.nytimes.com%2Finteractive%2F2019%2F12%2F19%2Fopinion%2Flocation-tracking-cell-phone.html&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710496649&sdata=P0H594btiGq6nzTdB6lwHV%2FWvf2D0%2Ba24oONHIHDCgE%3D&reserved=0) pall.

The Department of Defense is keenly aware that the proliferation of devices designed to track personal preferences, movement, location, and social networks is degrading personal anonymity and increasing targeting opportunities on their force. Individuals face persistent contact with an arsenal of data collection tools such as internet connected speakers, cameras with facial recognition, electronic passes used to pay transportation fares, license plate readers, home security systems and phone applications that track their lives. Simple vulnerabilities such as identifying as a military member on social media or being named in a news report are compounded when someone’s anonymity is being quietly stripped away through the examination their digital exhaust.

As a person’s data is being collected, stored, sold, resold and combined, patterns of life become discoverable. While much of this sold digital data is purportedly “sanitized” of personally identifying information, numerous reports demonstrate that it possible to reconstruct individual identity from metadata and through combination with other available data sources. As a result, a digital “pattern of life” can be used not only by companies, but by bad actors, be they criminals, or potentially, hostile governments as an act of terror or war.

As a result, the military has banned some electronic [devices](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.defense.gov%2FExplore%2FNews%2FArticle%2FArticle%2F1594486%2Fnew-policy-prohibits-gps-tracking-in-deployed-settings%2F&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710506644&sdata=z3CM3diokivVCxTsOHZBnGYhWf2Wkmoo413jLzj4oqA%3D&reserved=0) and [applications](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.nbcnews.com%2Ftech%2Ftech-news%2Fu-s-army-bans-tiktok-following-guidance-pentagon-n1109001&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C0%7C637160101710506644&sdata=OP2L3MnqZAR0UxZMd5bQ3QOhYmxqVyKD9Prm3YbUQrM%3D&reserved=0) that could be gathering data and is [educating](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fapps.dtic.mil%2Fdtic%2Ftr%2Ffulltext%2Fu2%2Fa549468.pdf-&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710516641&sdata=1OYmwPpETYn05StzyAV0lgW7d%2Bqbj48YLZWW68xoqU8%3D&reserved=0) service members of all ranks on good internet and social media [practices](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.arcyber.army.mil%2FPortals%2F34%2FFact%2520Sheets%2FDoD_Identity_Awareness_Protection_Management_Guide_March2019.pdf%3Fver%3D2019-06-24-174833-227&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710526636&sdata=OE9d4s%2BaxuTYd69oG39dp9soMCsr9GLZJqgGOxPzttk%3D&reserved=0). On Data Privacy Day, military twitter accounts urged individual users to be vigilant, frequently change passwords, and update social media privacy settings. While this kind of protection is important, individuals and families remain vulnerable to digital targeting, largely because vigilance is not sufficient when those associated with the military are particularly exposed to digital exploitation.

While there is some debate within the United States (in [Congress](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.latimes.com%2Fbusiness%2Ftechnology%2Fstory%2F2019-12-20%2Fnew-house-privacy-proposal-would-curb-data-collection-by-google-and-facebook&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C0%7C637160101710526636&sdata=IeH710Ttwn8qLrYL575wGvXhqz1qI0h1nmS0v%2FOnNFs%3D&reserved=0), the [Supreme Court](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.supremecourt.gov%2Fopinions%2F17pdf%2F16-402_new_o75q.pdf&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710536634&sdata=8ISArVd7bYHiGJTQFMw3SNV%2BWQqYMU2d9IA4BDDW5YY%3D&reserved=0), by the [ACLU](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ntia.doc.gov%2Ffiles%2Fntia%2Fpublications%2Faclu_comments_on_developing_the_administrations_approach_to_consumer_privacy.pdf&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710546629&sdata=Wo6KiV2Ee2bmDypozM16FfCpz4cSb5g%2B4R%2FppcWpJAk%3D&reserved=0)) and among its allies about the proper use of this technology and data, other nations, such as China, are using it to identify, track, and control their populations. If authoritarian regimes, some of whom build the very devices Americans are buying, are willing to use these tools against their own populations, we should expect they would be willing to use these tools, and the data extrapolated from them, to [target](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmwi.usma.edu%2Famerica-vs-russian-disinformation-societal-cohesion-empowered-institutions-can-win-war-fake-news%2F&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C0%7C637160101710546629&sdata=sb1kGh6tZAirHolfnGm2CZHrjhpnS3XhE25ag8fpACc%3D&reserved=0) their enemies. The vulnerabilities these devices are creating must be better understood if we are going to create a credible defense against an enemy inclined to exploit them.

Criminals have already demonstrated the ability to take advantage of these vulnerabilities. Cyberstalking and other cyber threats are on the rise and connected devices give more opportunity and gateways to gather data and more vectors for harassment. These criminal [cases](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.justice.gov%2Fusao%2Ffile%2F851856%2Fdownload&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C0%7C637160101710556623&sdata=dH1BL7j9bE7vm2o9asRcOojKnGDB%2FW6EDs4TWcsZqZI%3D&reserved=0) demonstrate that the means exist to stalk and harass individuals through email, text, call, doxing, and surveillance through GPS, cameras, and smart TVs . Many threats go unreported, and police departments are struggling to understand the scope and find the means to effectively stop these complex, multi-jurisdictional crimes. This struggle is a harbinger of things to come in the world of national security.

Unfortunately, it is easy to imagine a near-future in which military family members are digitally stalked, the cameras in their homes hacked, their personal data stolen, shared or ransomed. Imagine the fear that could be inflicted if the patterns of life of just a handful of family members are discovered and suddenly someone is talking from their speakers, changing the temperature in their home, posting their photos, publishing their address, cutting off their internet, or broadcasting a child’s bedroom camera to a deployed parent. Any of these things are technically possible right now. Now imagine this being done on a wide scale with much more serious threats and results.

Risk mitigation must begin immediately. While the Department of Defense should support broad congressional debate on data privacy legislation, the military has a unique challenge in this arena. Military family members are often living off military installations and generally fall outside the jurisdiction of military authorities. The tremendous assets that U.S. Cyber Command has at its disposal can work to inform military members and their families about the threat and how make themselves a [harder](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.arcyber.army.mil%2FPortals%2F34%2FFact%2520Sheets%2FDoD_Identity_Awareness_Protection_Management_Guide_March2019.pdf%3Fver%3D2019-06-24-174833-227&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C1%7C637160101710566619&sdata=fzjbtCoqn9%2FHPh4SvUze1wtqvG8cDPXHGOV3o3lX9Y0%3D&reserved=0) target, but it will likely fall to law enforcement authorities to, at least initially, deal with these threats and the immediate results.

First, the military must be aware of these attacks, which are likely to occur outside of their jurisdiction. This requires an expansion its current suspicious activity reporting campaigns to include cyber incidents. These military “See Something, Say Something” campaigns serve a twofold purpose: to inform the public of the threat and to ensure suspicious activity is reported. Additionally, current anonymous criminal reporting tools must also highlight the ability to report cybercrimes. Anonymous reporting capabilities may increase the likelihood of capturing information on typically under-reported crimes, like cybercrimes, thus improving the ability to mitigate damage or prevent a further attack.

Once aware of a potential threat, military law enforcement organizations should be DoD’s lead on tracking them. Illicit cyber activities are generally considered criminal incidents, therefore Army and Marine Corps Criminal Investigation Division, Air Force Office of Special Investigation, and Naval Criminal Investigative Services, are best suited to deal with them. All these agencies have some cyber capability and routinely deal with other law enforcement agencies over matters of jurisdiction. Military law enforcement would function as the sensors, then military or other federal cyber and intelligence organizations could act within their authorities to mitigate the threat.

Geographic distance has long afforded the United States a safe and assured homefront, but the digital world affords no such luxury. Data is being dispersed at an alarming rate and in the near future, could have a significant impact on national security. Currently, this vulnerability is unfairly carried by the individual. Meanwhile, the companies who design the technology and gather data are largely profiting from this personal risk. As the [debate](https://nam04.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cnas.org%2Fpublications%2Fcommentary%2Fthe-national-security-imperative-of-protecting-user-data&data=02%7C01%7Cmgruss%40mco.com%7Ceabbaa8e295c4cc8503d08d7a5bc95e4%7C1d5c96e57ee2446dbed8d0f8c50edea5%7C1%7C0%7C637160101710566619&sdata=%2BAbXpGiurFna7w89Ph2yTuqn1zQfJZdH7JyuvBhAA3A%3D&reserved=0) over privacy continues, it is important to keep in mind the unique impact digital footprints may have on the safety and security of our military personnel and their families.

*Col. Sarah Albrycht is a senior military fellow at the Center for a New American Security. The views expressed are those of the author and do not reflect the official position of the Department of the Army or Department of Defense or the U.S. government.*

Close