



# Insider Threat Risk in Afghanistan

## Spatial Analysis of Counterintelligence Force Distribution for an Enduring Troop Presence: 2013 - 2017



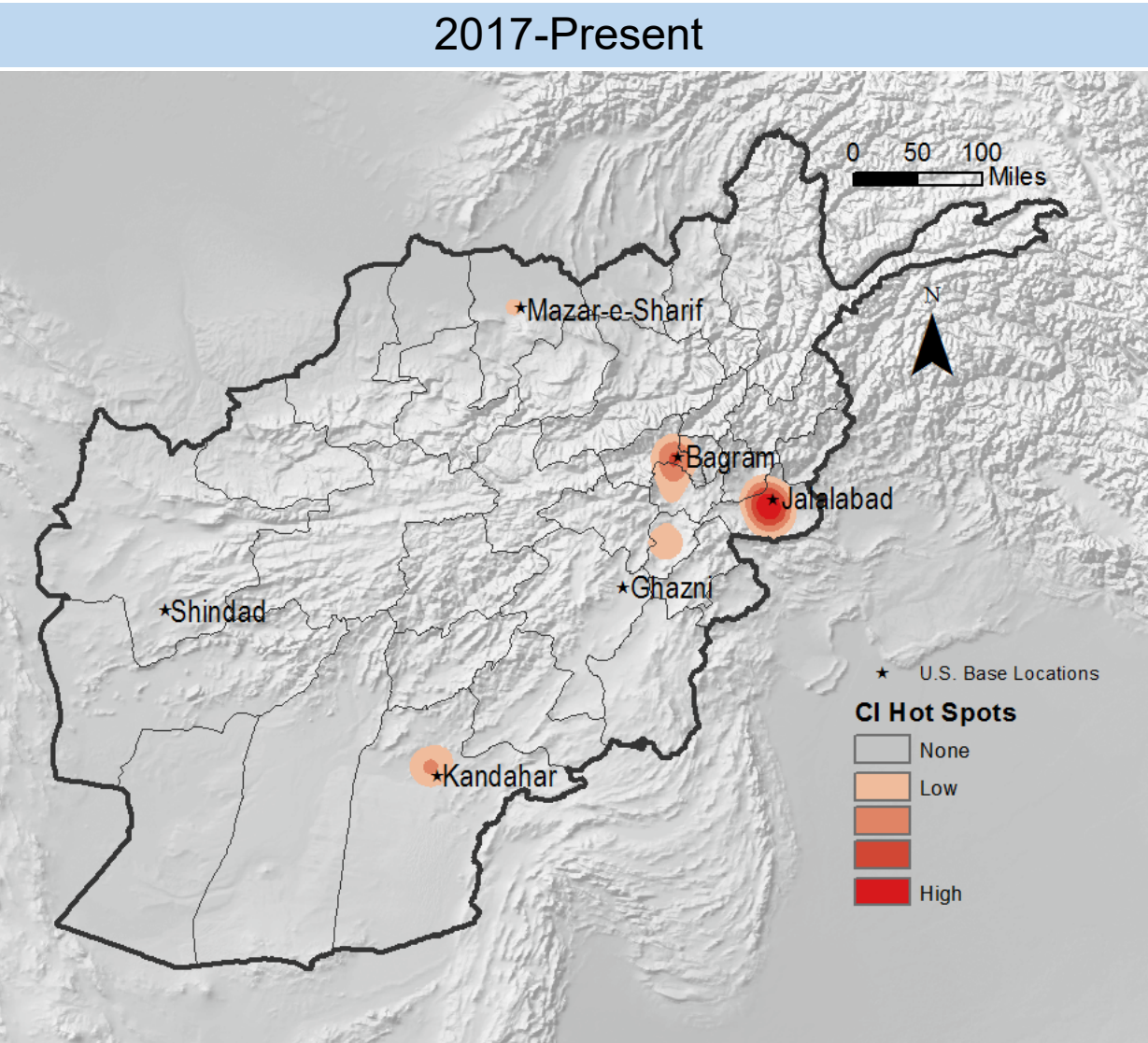
### Annual Counterintelligence Threat Activity

Historical Counterintelligence (CI) threats are a very important factor in determining the risk of future attacks. However, one must consider the environment that may have shaped CI patterns. CI hot spots only loosely correlate with overall terrorist activity. Many terrorist attacks are directed against the local population, local police and the Afghan National Army. This analysis only includes CI activity that is directed at NATO forces.

From January 2013 to December 2014, CI activity was high across Afghanistan, as the allied troop presence was large and NATO forces dispersed across the country to support the presidential elections. The large hot spot west of Kandahar reflects the activity around Helmand base, which closed in the later half of 2014.

From January 2015 to December 2016, CI activity was low around all bases, except for Bagram. This is likely due to the withdrawal of most major combat forces in the later half of 2014. CI incidents in Bagram increased, perhaps due to the fact that many allied personnel left the country through Bagram's air field, therefore increasing allied troop presence there. It may also be the result of additional allied presence in Kabul, tasked with protecting the newly elected Afghan administration.

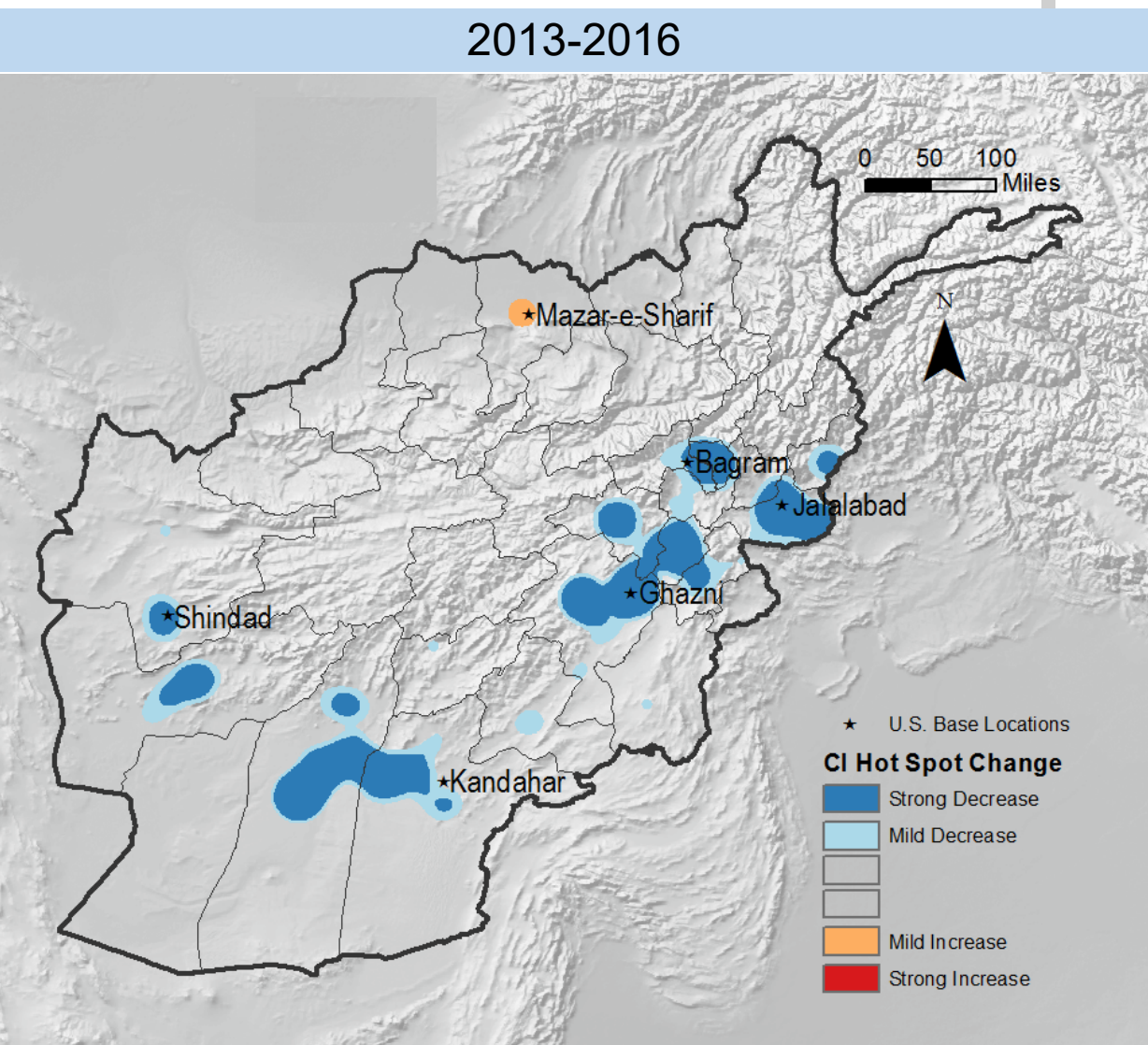
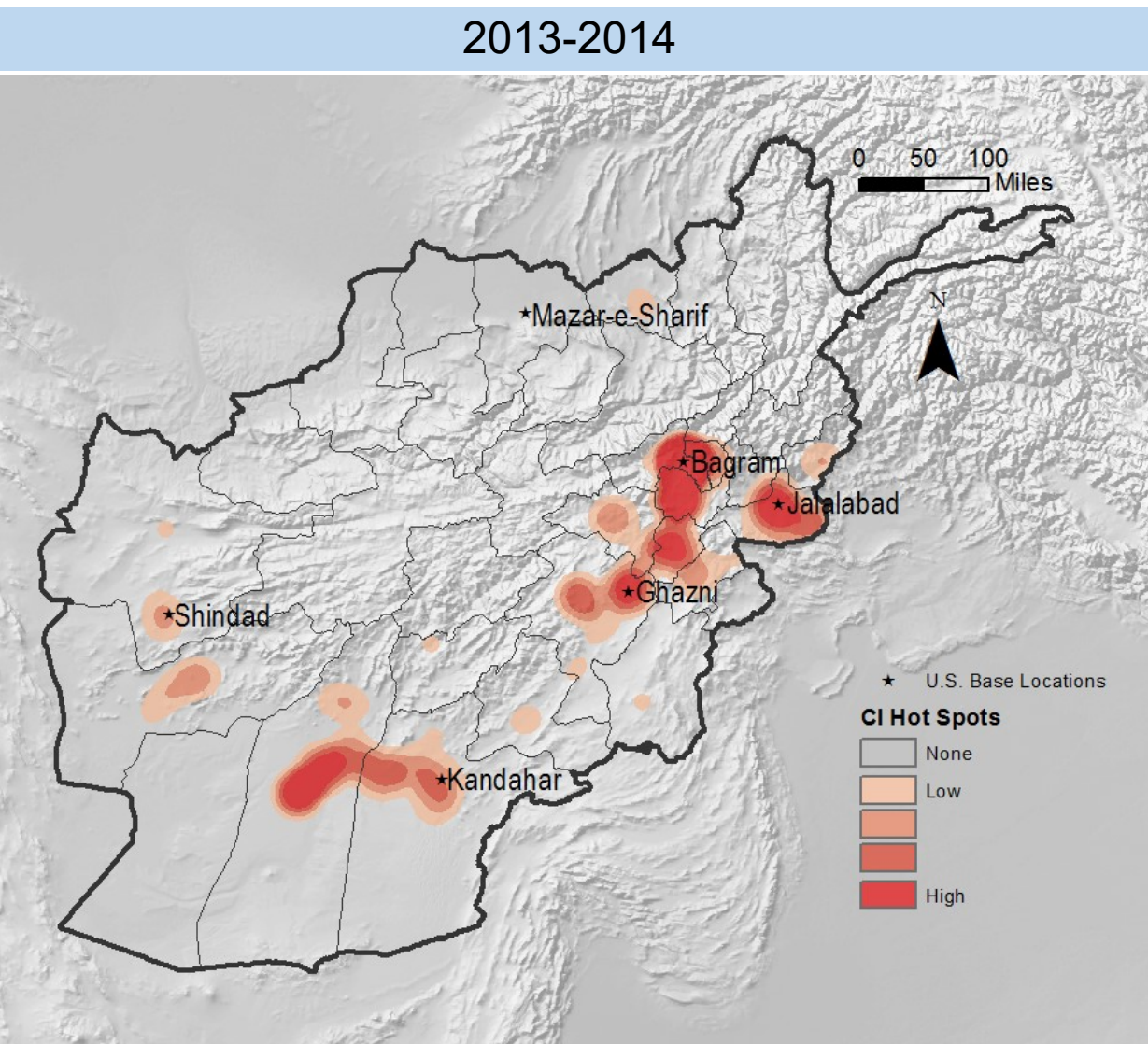
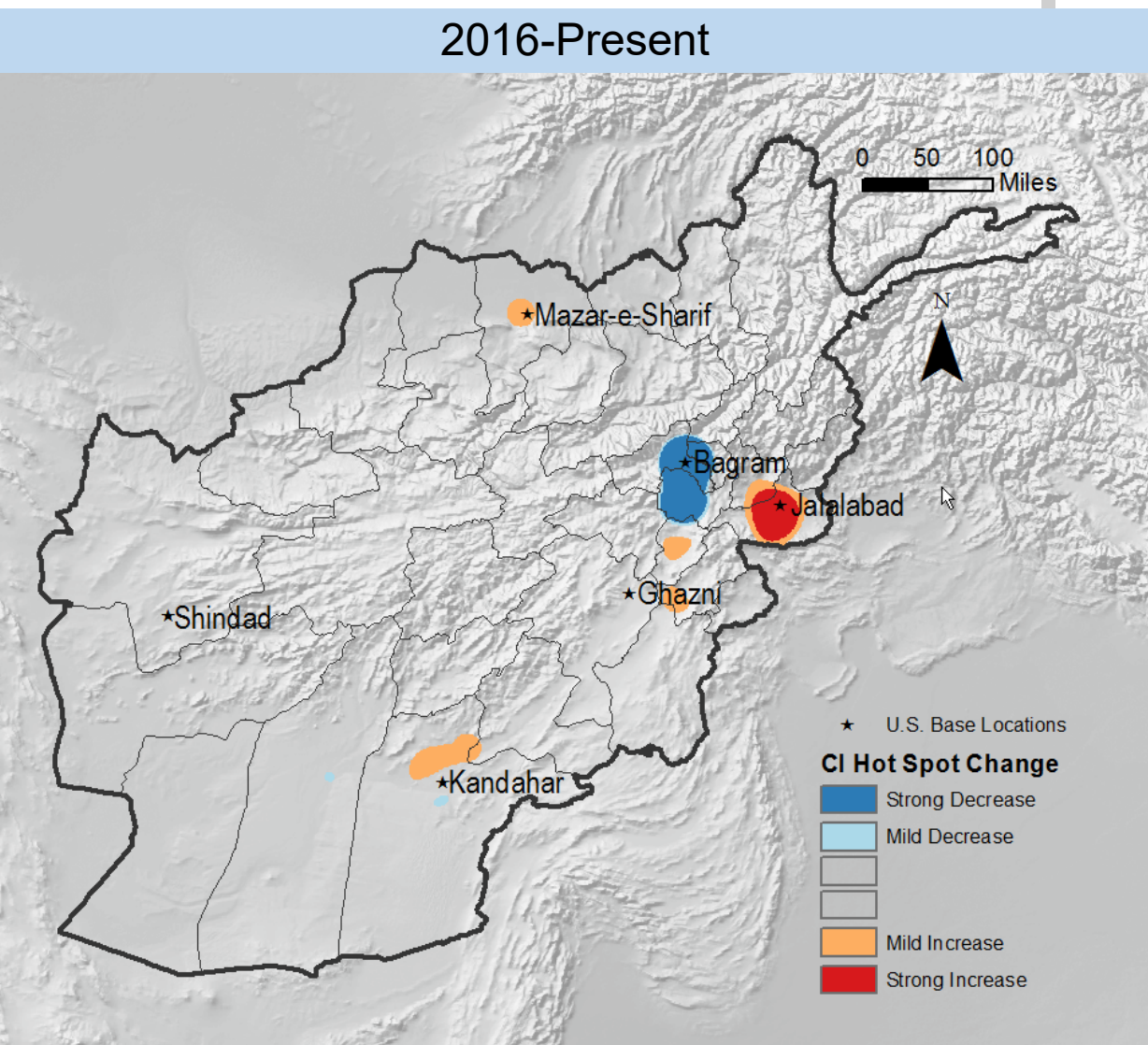
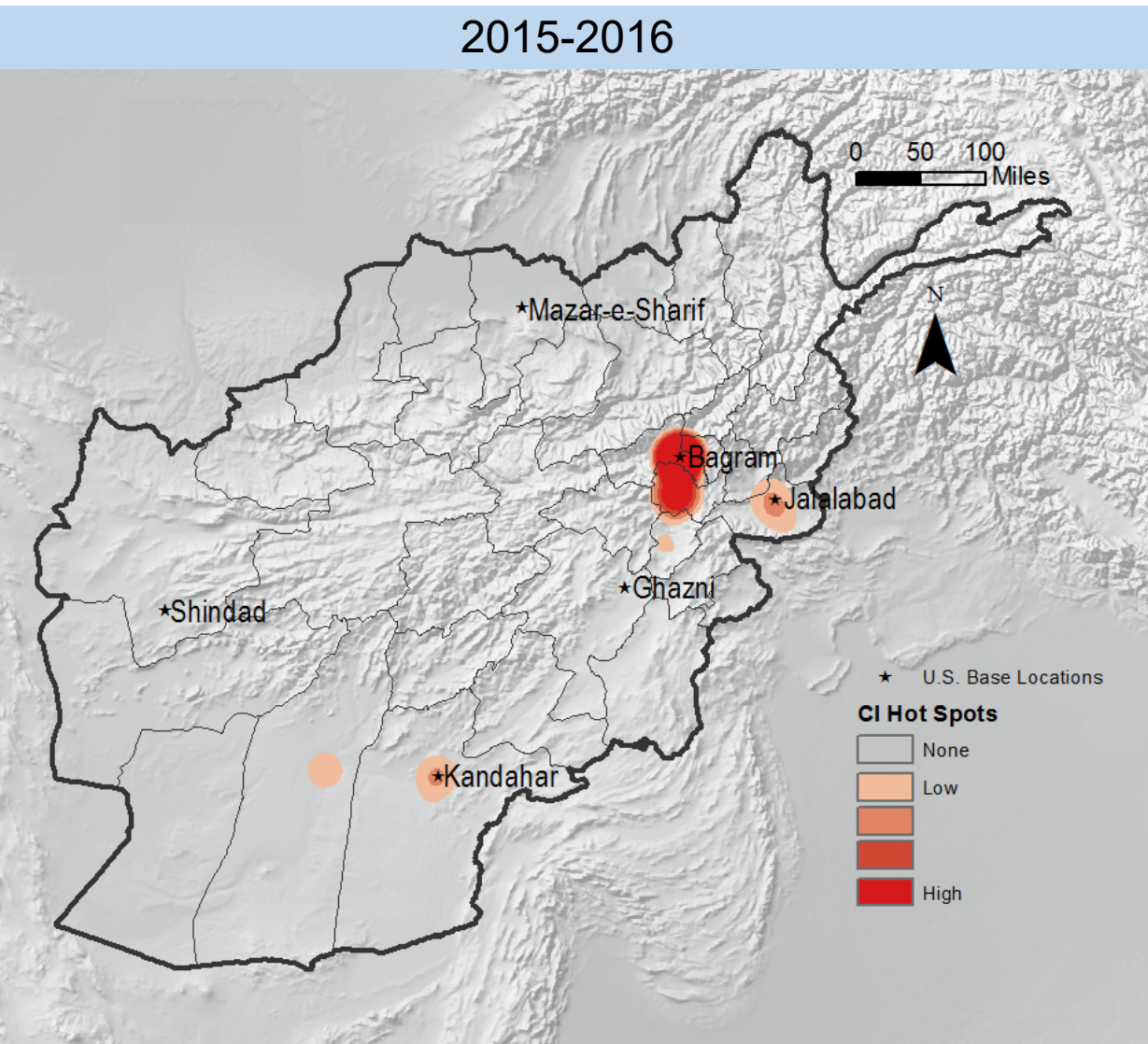
Since 2017, CI activity was highest in Jalalabad. While the exact location of U.S. forces and their activity is classified, the new U.S. administration announced plans to increase the presence of trainers and advisors in Afghanistan. The increase of CI activity around Jalalabad may be an indication that the area has become a focus for the enduring presence in Afghanistan and that there is increased interaction between local nationals and allied forces. Train and assist missions require daily interaction between the two forces. The increased access to allied forces also increases the risk of potential attack.



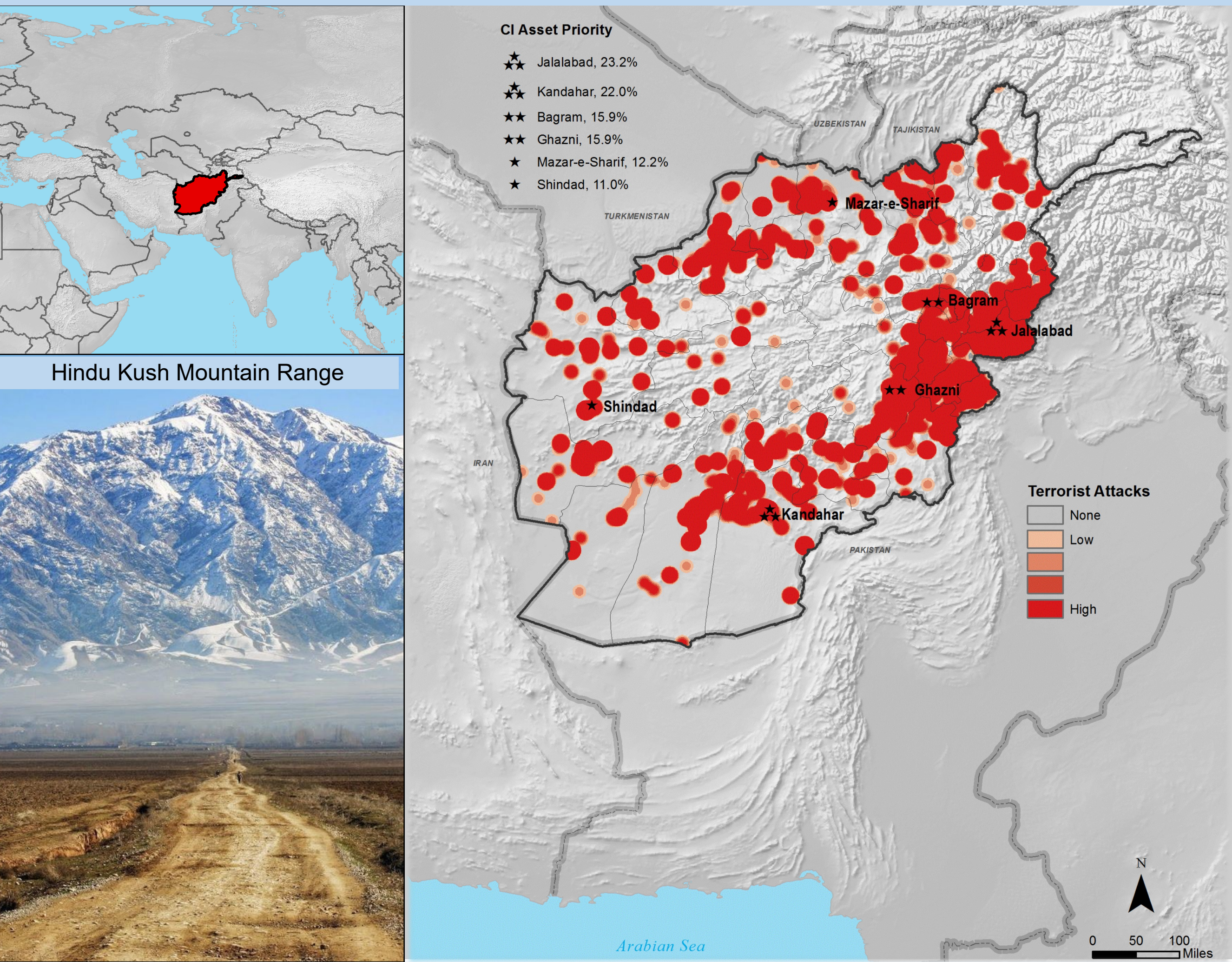
### Counterintelligence Threat Change Patterns

Between 2013-2016, CI incidents decreased substantially with the withdrawal of most major combat forces in 2014. All areas showed reduced CI activity. The large decrease west of Kandahar is due to the Helmand base-closure.

Since 2016, CI activity in and around Bagram (in vicinity of Kabul) has decreased as well, likely due to reduced foreign troop presence in that area and effectiveness of local national security forces. However, Jalalabad, along the Pakistani border, has seen a strong increase in insider incidents.



### All Terrorist Attack zones since 2015 and recommended Counterintelligence prioritization

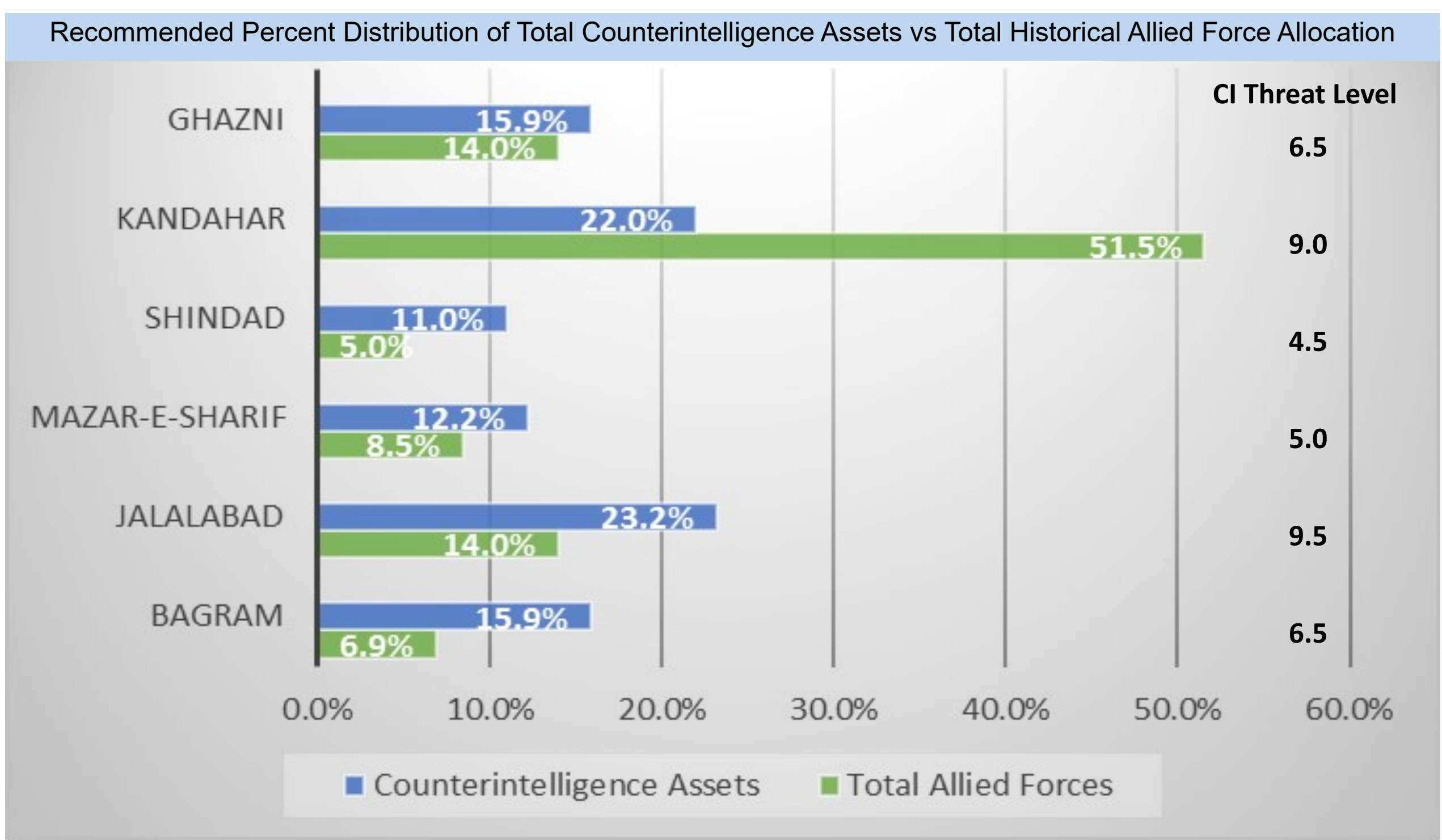


### Recommended Prioritization for Counterintelligence (CI) Assets

Since 2001, NATO involvement in Afghanistan has claimed the lives of thousands of coalition soldiers. Historically, counterintelligence assets have deployed with their assigned ground units. As a result, the relationship of counterintelligence operators remains relatively constant to that of the total allied force they support. When a particular unit experiences an increased CI threat, they may ask for additional support. Unfortunately, in the case of counterintelligence issues, this is often retro-active. A request for additional support usually originates as a result of an insider attack, which include acts of sabotage, espionage and assassinations.

On 30 January, 2018, during his State of the Union address, the President of the United States announced an enduring U.S. troop presence in Afghanistan, with no planned date for withdrawal. As of April, 2018, eleven thousand U.S. troops and additional NATO forces are deployed in the country as trainers and advisors, with the possibility of more forces arriving in the future. The continued interaction will once again make counterintelligence efforts a priority. CI work cannot be done from behind an office desk, and with limited resources available, planners have to pre-empt the need for CI specialists based on the allied bases that are at the greatest risk.

This project developed CI threat levels for each operational NATO base and distributed CI forces accordingly. The threat vulnerability matrix is a combination of several factors, including the number of allied forces at the base, historical CI incidents, the recent change patterns in CI incidents and population patterns that relate to CI risk.



### U.S. and Afghan Soldier Taking a Break



While the vast majority of interactions between Afghan and allied forces is positive, there have been a number of instances in which locals turn on their foreign partners. These instances lead to distrust and degrade mission effectiveness. Counterintelligence operators are responsible for finding and removing these threats.

### Population Patterns with Counterintelligence Applications

Population patterns are an often overlooked but very important clue into determining the risk of insider attacks. While none of the three population variables used in this analysis are very significant on their own, the combination could increase the CI threat level of an allied base.

High population density makes it a lot more challenging to determine possible threats. People living in these areas often moved from elsewhere in the country in their search for work, sometimes multiple times. As a result, they have a much larger and more complex social network. This makes it more difficult for CI operators to determine which social group or groups an individual is most closely connected with. On the other hand, bases located in rural areas provide a level of security. Individuals with abnormal or risky social connections stand out and can be subjected to more scrutiny or removed from access to allied bases. Bagram is in the most densely populated area, with Ghazni and Jalalabad also located near urban areas.

Pashtuns are Afghanistan's dominant ethnicity, they are statistically also more likely to commit insider attacks. This is due to the fact that the Taliban is mostly made up of Pashtuns, especially the leadership. On the other hand, anti-Taliban militia are often Uzbek or Tajik. Because Pashtuns often have familial relations to members of the Taliban, they are easily influenced and pressured into conducting insider attacks. Kandahar, Ghazni and Jalalabad are at the highest risk, while Bagram and Shindad are surrounded by Pashtu areas.

Females are not permitted to work with allied forces, for the most part. Afghan army, local national security forces and local workers on allied bases are almost exclusively male. However, most of Afghanistan has a fairly even distribution of male to female ratios, making this only a very small factor. Furthermore, most bases are located outside areas that are predominantly male, with the exception of Kandahar.

### Allied Troop Levels

A significant factor in the risk of CI attacks is the size of the potential target, in other words, the number of allied troops at each base. Where there are no allied troops, there is not CI threat. While troop level distribution is classified, this analysis used 2010 troop levels, to estimate the possible percent distribution of future deployments.

