

```
In [1]: import nltk
```

```
In [2]: Paragraph = '''The U.S. national security apparatus has cautioned that one avenue
```

In [3]: Paragraph

The U.S. national security apparatus has cautioned that one avenue for retaliation Iran is likely to attacks targeting the U.S. public and private sectors. The day after Soleimani's killing, the Department of Homeland Security issued a bulletin warning that while it did not have information about an imminent attack, "Iran maintains a capability to conduct cyber attacks against the United States. Iran is capable, at a minimum, of carrying out attacks with the potential to damage critical infrastructure in the United States." Such an attack could further "come with little or no warning." The Department of Cybersecurity and Infrastructure Security Agency (CISA) within DHS issued an alert to stakeholders in the private sector, maintaining a heightened state of awareness and increased organizational vigilance, urging cybersecurity personnel to monitor for Iranian indicators of compromise and tactics, techniques, and procedures." The FBI similarly issued a bulletin to U.S. companies on January 9, 2020, assessing that Iranian hackers could use "a range of computer networks and technologies to conduct attacks in retaliation for last week's strikes against Iranian military leadership." The FBI advised companies to monitor for Iranian "cyber reconnaissance activity" since the Soleimani killing and offered technical advice on how to protect networks from efforts to exploit vulnerabilities in virtual private network (VPN) applications, which Iran has historically used to access computer networks allowing it to monitor, exfiltrate, and potentially destroy sensitive data. The FBI also noted that "Iran has issued by the U.S. intelligence community for several years, warning of Iran's determination and ability to conduct cyber attacks against the U.S. and its allies. The 2018 Worldwide Threat Assessment of the U.S. Intelligence Community noted that Iran is working to penetrate U.S. and Allied networks for espionage and to position itself for potential future attacks. It further warned that Iran is growing increasingly aggressive and will only be further emboldened absent a clear deterrence of its malign cyber activities. According to the assessment, "The use of cyber attacks as a foreign policy tool has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing the boundaries and pose growing threats to the United States and US partners." The 2019 Worldwide Threat Assessment noted that Iran has entered a new phase, with Iran increasingly focused on deploying "cyber attack capabilities that would be used to target critical infrastructure in the United States and allied countries." At this point, Iranian cyber attacks are capable of causing significant effects – such as disrupting a large company's corporate networks for days to weeks." The 2020 Worldwide Threat Assessment of the U.S. Intelligence Community notes that the Iranian cyber threat has advanced further, as Iran has now acquired "the ability to conduct attacks against U.S. and Allied networks as to conduct influence and espionage activities." The mounting concerns over an Iranian cyber attack have led to increased vigilance. Iran has made in advancing its cyber warfare capabilities over the past decade. In 2010, over 15 Iranian computers were infected by the Stuxnet computer virus, a worm jointly developed by the U.S. and Israel that destroyed nearly 1,000 centrifuges at the weakness of Iran's cyber defenses, leading Iran to accelerate the advancement of offensive and defensive capabilities. By March 2012, Iran created a "cyber command" known as the Supreme Council of Cyberspace, comprised of senior officials. The council acts as a unified command tasked with coordinating Iran's cybersecurity and plotting cyber operations.'

```
In [4]: import re
        from nltk.corpus import stopwords
        from nltk.stem.porter import PorterStemmer
        ##from nltk.stem import WordNetLemmatizer
        from nltk.tokenize import word_tokenize
        Paragraph_tokens = word_tokenize(Paragraph)
        ps = PorterStemmer()
        #wordnet=WordNetLemmatizer()
        sentences = nltk.sent_tokenize(Paragraph )
```

```
In [6]: corpus = []
        for i in range(len(sentences)):
            review = re.sub('[^a-zA-Z]', ' ', sentences[i])
            review = review.lower()
            review = review.split()
            # review = [wordnet.Lemmatize(word) for word in review if not word in set(stopwords)]
            review = ' '.join(review)
            corpus.append(review)
```

In [7]: corpus

```
['the u s national security apparatus has cautioned that one avenue for retaliation iran is likely to
attacks targeting the u s public and private sectors',
 'the day after soleimani s killing the department of homeland security dhs issued a bulletin warning
on about an imminent attack iran maintains a robust cyber program and can execute cyber attacks again:
 'iran is capable at a minimum of carrying out attacks with temporary disruptive effects against crit:
tes such an attack could further come with little or no warning several days later the cybersecurity :
sa within dhs issued an alert to stakeholders in the u s cybersecurity community recommending a height
d organizational vigilance urging cybersecurity personnel to immediately flag any known iranian indic:
iques and procedures',
 'the fbi similarly issued an advisory obtained by cyberscoop to u s companies on january assessing tl
of computer network operations against u s based networks in retaliation for last week s strikes again:
bi advisory noted that there had been an uptick in iranian cyber reconnaissance activity since the so:
advice to companies on thwarting iranian efforts to exploit vulnerabilities in virtual private network:
torically used to gain a foothold in computer networks allowing it to monitor exfiltrate and potentia:
 'the fbi and dhs advisories echoed assessments issued by the u s intelligence community for several y
and ability to launch offensive cyber attacks against the u s and its allies',
 'the worldwide threat assessment of the u s intelligence community concluded that iran will continue
networks for espionage and to position itself for potential future cyber attacks the assessment furthe:
singly aggressive and will only be further emboldened absent significant push back against its malign
 'according to the assessment the use of cyber attacks as a foreign policy tool outside of military co:
oradic lower level attacks',
 'russia iran and north korea however are testing more aggressive cyber attacks that pose growing thre:
ners the worldwide threat assessment noted that the iranian cyber threat had entered a new phase with
ng cyber attack capabilities that would enable attacks against critical infrastructure in the united :
oint iranian cyber attacks are capable of localized temporary disruptive effects such as disrupting a
or days to weeks the worldwide threat assessment found that the iranian cyber threat has advanced fur:
lity to conduct attacks on critical infrastructure as well as to conduct influence and espionage activ:
 'the mounting concerns over an iranian cyber attack reflect the considerable investment iran has made
bilities over the past decade',
 'in over iranian nuclear facilities were targeted by the stuxnet computer virus a worm jointly develo:
oyed nearly centrifuges',
 'the attack exposed the weakness of iran s cyber defenses leading iran to accelerate the advancement
fare capabilities',
 'by march iran created a cyber command known as the supreme council of cyberspace comprised of senior
s',
 'the council acts as a unified command tasked with coordinating iran s cybersecurity and plotting out
operations']
```

In [9]: review

```
'the council acts as a unified command tasked with coordinating iran s cybersecurity and plotting out
perations'
```

In [11]: Paragraph\_tokens

```
'Security',  
'Agency',  
'(',  
'CISA',  
)',  
'within',  
'DHS',  
'issued',  
'an',  
'alert',  
'to',  
'stakeholders',  
'in',  
'the',  
'U.S.',  
'cybersecurity',  
'community',  
'recommending',  
'a',  
'heightened',  
'state',  
'of',  
'awareness',  
'and',  
'increased'.
```

In [12]: sentences

['The U.S. national security apparatus has cautioned that one avenue for retaliation Iran is likely to use is cyber attacks targeting the U.S. public and private sectors.',

'The day after Soleimani's killing, the Department of Homeland Security (DHS) issued a bulletin warning about an imminent attack, "Iran maintains a robust cyber program and can execute cyber attacks :

'Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure." Such an attack could further "come with little or no warning." Several days later, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS issued an alert to stakeholders in the U.S. cybersecurity community recommending increased organizational vigilance, urging cybersecurity personnel to immediately flag "any known tactics, techniques, and procedures.".',

'The FBI similarly issued an advisory, obtained by Cyberscoop, to U.S. companies on January 9, 2020, advising them to use "a range of computer network operations against U.S.-based networks in retaliation for last week's cyberattacks." The FBI advisory noted that there had been an uptick in Iranian "cyber reconnaissance activities." The advisory also offered technical advice to companies on thwarting Iranian efforts to exploit vulnerabilities in virtual machines, which Iran has historically used to gain a foothold in computer networks allowing it to monitor, exfiltrate, and delete sensitive data.',

'The FBI and DHS advisories echoed assessments issued by the U.S. intelligence community for several years warning of Iran's "onion" capability and ability to launch offensive cyber attacks against the U.S. and its allies.',

'The 2018 Worldwide Threat Assessment of the U.S. Intelligence Community concluded that Iran "will continue to use its cyber capabilities to target Allied networks for espionage and to position itself for potential future cyber attacks." The assessment also noted that Iran is becoming increasingly aggressive and will only be further emboldened absent significant push back against its activities.',

'According to the assessment, "The use of cyber attacks as a foreign policy tool outside of military operations is still in its early stages, but it is becoming more sporadic lower-level attacks.',

'Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing concerns to U.S. allies and partners." The 2019 Worldwide Threat Assessment noted that the Iranian cyber threat had entered a new phase, moving from "localized, temporary disruptive effects - such as disrupting corporate networks for days to weeks." The 2020 Worldwide Threat Assessment found that the Iranian cyber threat has now acquired "the ability to conduct attacks on critical infrastructure, as well as to conduct large-scale attacks.".',

'The mounting concerns over an Iranian cyber attack reflect the considerable investment Iran has made in its cyber capabilities over the past decade.',

'In 2010, over 15 Iranian nuclear facilities were targeted by the Stuxnet computer virus, a worm joint effort by the U.S. and Israel that destroyed nearly 1000 centrifuges.',

'The attack exposed the weakness of Iran's cyber defenses, leading Iran to accelerate the advancement of its cyber capabilities.',

'By March 2012, Iran created a "cyber command" known as the Supreme Council of Cyberspace, comprised of senior government officials.',

'The council acts as a unified command tasked with coordinating Iran's cybersecurity and plotting offensive cyber operations.']

```
In [13]: from nltk.tokenize import WordPunctTokenizer
# Create a WordPunctTokenizer
tokenizer = WordPunctTokenizer()
# Tokenize using the WordPunctTokenizer
Paragraph_wordpunct = tokenizer.tokenize(Paragraph)
# Print the tokenized version
print(Paragraph_wordpunct)
```

[ 'The', 'U', '.', 'S', '.', 'national', 'security', 'apparatus', 'has', 'cautioned', 'that', 'one', 'is', 'likely', 'to', 'pursue', 'is', 'launching', 'offensive', 'cyber', 'attacks', 'targeting', 'and', 'private', 'sectors', '.', 'The', 'day', 'after', 'Soleimani', 's', 'killing', 'the', 'curity', '(', 'DHS', ')', 'issued', 'a', 'bulletin', 'warning', 'that', 'while', 'it', 'did', 'not', 'imminent', 'attack', 'Iran', 'maintains', 'a', 'robust', 'cyber', 'program', 'and', 'can', 'not', 'the', 'United', 'States', '.', 'Iran', 'is', 'capable', 'at', 'a', 'minimum', 'of', 'temporary', 'disruptive', 'effects', 'against', 'critical', 'infrastructure', 'in', 'the', 'United', 'K', 'could', 'further', 'come', 'with', 'little', 'or', 'no', 'warning', 'Several', 'days', 'y', 'and', 'Infrastructure', 'Security', 'Agency', '(', 'CISA', ')', 'within', 'DHS', 'issued', 'an', 'the', 'U', '.', 'S', '.', 'cybersecurity', 'community', 'recommending', 'a', 'heightened', 'state', 'd', 'organizational', 'vigilance', 'urging', 'cybersecurity', 'personnel', 'to', 'immediately', 'n', 'indicators', 'of', 'compromise', 'and', 'tactics', 'techniques', 'and', 'procedures', 'sued', 'an', 'advisory', 'obtained', 'by', 'Cyberscoop', 'to', 'U', '.', 'S', '.', 'companies', 'assessing', 'that', 'Iranian', 'hackers', 'could', 'use', 'a', 'range', 'of', 'computer', 'U', '.', 'S', 'based', 'networks', 'in', 'retaliation', 'for', 'last', 'week', 's', 's', 'tary', 'leadership', 'The', 'FBI', 'advisory', 'noted', 'that', 'there', 'had', 'been', 'an', 'r', 'reconnaissance', 'activity', 'since', 'the', 'Soleimani', 'killing', 'and', 'offered', 'tech', 'on', 'thwarting', 'Iranian', 'efforts', 'to', 'exploit', 'vulnerabilities', 'in', 'virtual', 'private', 'ications', 'which', 'Iran', 'has', 'historically', 'used', 'to', 'gain', 'a', 'foothold', 'in', 'it', 'to', 'monitor', 'exfiltrate', 'and', 'potentially', 'destroy', 'sensitive', 'data', 'isories', 'echoed', 'assessments', 'issued', 'by', 'the', 'U', '.', 'S', '.', 'intelligence', 'communi', 'warning', 'of', 'Iran', 's', 'determination', 'and', 'ability', 'to', 'launch', 'offensive', 'cy', 'U', '.', 'S', '.', 'and', 'its', 'allies', 'The', '2018', 'Worldwide', 'Threat', 'Assessment', 'elligence', 'Community', 'concluded', 'that', 'Iran', 'will', 'continue', 'working', 'to', 'penet', 'llied', 'networks', 'for', 'espionage', 'and', 'to', 'position', 'itself', 'for', 'potential', 'future', 'assessment', 'further', 'warned', 'that', 'Iran', 'is', 'growing', 'increasingly', 'aggressive', 'anc', 'emboldened', 'absent', 'significant', 'push', 'back', 'against', 'its', 'malign', 'cyber', 'activitie', 'assessment', 'The', 'use', 'of', 'cyber', 'attacks', 'as', 'a', 'foreign', 'policy', 'tool', 'lict', 'has', 'been', 'mostly', 'limited', 'to', 'sporadic', 'lower', 'level', 'attacks', 'F', 'rth', 'Korea', 'however', 'are', 'testing', 'more', 'aggressive', 'cyber', 'attacks', 'that', 'o', 'the', 'United', 'States', 'and', 'US', 'partners', 'The', '2019', 'Worldwide', 'Threat', 'Iranian', 'cyber', 'threat', 'had', 'entered', 'a', 'new', 'phase', 'with', 'Iran', 'increasingl', 'cyber', 'attack', 'capabilities', 'that', 'would', 'enable', 'attacks', 'against', 'critical', 'd', 'States', 'and', 'allied', 'countries', 'At', 'this', 'point', 'Iranian', 'cyber', 'att', 'localized', 'temporary', 'disruptive', 'effects', 'such', 'as', 'disrupting', 'a', 'large', 'networks', 'for', 'days', 'to', 'weeks', 'The', '2020', 'Worldwide', 'Threat', 'Assessment', 'I', 'ber', 'threat', 'has', 'advanced', 'further', 'as', 'Iran', 'has', 'now', 'acquired', 'the', 's', 'on', 'critical', 'infrastructure', 'as', 'well', 'as', 'to', 'conduct', 'influence', 'and', 'he', 'mounting', 'concerns', 'over', 'an', 'Iranian', 'cyber', 'attack', 'reflect', 'the', 'considerat', 'ade', 'in', 'advancing', 'its', 'cyber', 'warfare', 'capabilities', 'over', 'the', 'past', 'decade', 'Iranian', 'nuclear', 'facilities', 'were', 'targeted', 'by', 'the', 'Stuxnet', 'computer', 'virus', 'ed', 'by', 'the', 'U', '.', 'S', '.', 'and', 'Israel', 'that', 'destroyed', 'nearly', '1000', 'centrif', 'd', 'the', 'weakness', 'of', 'Iran', 's', 'cyber', 'defenses', 'leading', 'Iran', 'to', 'acc', 'f', 'offensive', 'and', 'defensive', 'cyber', 'warfare', 'capabilities', 'By', 'March', '2012', 'ber', 'command', 'known', 'as', 'the', 'Supreme', 'Council', 'of', 'Cyberspace', 'comprised', 'intelligence', 'officials', 'The', 'council', 'acts', 'as', 'a', 'unified', 'command', 'tasked', 's', 'cybersecurity', 'and', 'plotting', 'out', 'of', 'offensive', 'and', 'retaliatory', 'cyber',

```
In [14]: # Create the wordcloud object  
# Libraries  
from wordcloud import WordCloud  
import matplotlib.pyplot as plt  
# Create the wordcloud object  
wordcloud = WordCloud(width=480, height=480, margin=0).generate(Paragraph)  
# Display the generated image:  
plt.imshow(wordcloud, interpolation='bilinear')  
plt.axis("off")  
plt.margins(x=0, y=0)  
plt.show()
```